WS410 User Manual

Rev 1.1.0, October 2007

Copyright Notice

©2007 Wavion, Inc. All rights reserved. Wavion is a registered trademark of Wavion in the United States and certain other jurisdictions. Specifications are subject to change without notice. Loctite is a registered trademark of Loctite Corporation, USA.

FCC Notice to Users and Operators

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by using one of the folowing measures:

- Reorient or relocate the receiving antenna.
- Increase separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician.

This Part 15 radio device operates on a non-interference basis with other devices operating at this frequency. Any changes or modification to said product not expressly approved by Wavion could void the user's authority to operate this device.

WARNING: It is illegal to modify the construction of this product. Modifying the operating frequency or enhancing the transmit output power through the use of external amplifiers or other equipment is specifically disallowed by the "Telecommunications Act."

WARNING: This device is for outdoor use with conditions that no harmful interference to authorized radio stations results from the operation of this device. This device shall not influence aircraft security and/or interfere with legal communications as defined in the "Telecommunications Act." If this device is found to cause interference, the operator of this equipment shall cease operating this device immediately until no interference is achieved.

NOTE: This device must be installed by a trained professional, value added reseller or systems integrator who is familiar with RF planning issues and the regulatory limits in the United States of America.

READ THIS FIRST!

Important Safety Instructions

CAUTION: The exclamation point within a triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the product.

WARNING: The lightning flash with an arrowhead symbol within a triangle is intended to alert the user to the presence of uninsulated ìdangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

CAUTION: Read and save these instructions. Heed all warnings. Follow all instructions.

CAUTION: Do not defeat the safety purpose of the grounding. Only use attachments/ accessories specified by the manufacturer.

CAUTION: Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way. For example, if the power-supply cord or plug is damaged, liquid has been spilled on the apparatus, objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, it does not operate normally, or has been dropped.

WARNING: There is a risk of personal injury or death if the WS-410 antennas come near electric power lines. Carefully read and follow all instructions in this manual. By nature of the installation, you may be exposed to hazardous environments and high voltage. Use caution when installing the outdoor system.

WARNING: This apparatus must be connected to earth ground.

WARNING: Do not open the unit. There is a risk of electric shock inside.

CAUTION: You are cautioned that any change or modification not expressly approved in this manual could void your authority to operate this equipment.

CAUTION: There are no user-serviceable parts inside. All service must be performed by qualified personnel.

CAUTION: The RJ45 connectors of your Wavion WS-410 may source DC power on pins 4,5 and 7,8. The IEE 802.3 standards allow for pins 4,5 and 7,8 to be used for Power Over Ethernet. Some products may be incompatible with the Wavion Power Over Ethernet capability. If such problems occur, make sure that the unit is configured with the Power Over Ethernet capability set to Off (default setting). If problems persist, use Ethernet cables that have no connections to the unused pins 4,5 and 7,8.

CAUTION: The Wavion WS410 can be installed in wet, outdoor locations. Make sure closure caps are installed and all cable connections are securely fastened and waterproofed.

CAUTION: The Wavion WS410 can only be used with approved antennas.

About This Manual

The following describes configuration of the WS410. It is intended for use by network engineers and administrators charged with setting up and administering Wavion wireless networks. Them manual contains the following:

- Chapter 1: Using the WS410 Graphical User Interface on page 10: Introduces the WS410, describes the application page and menu bar, and how to navigate through the system.
- Chapter 2: Viewing the System Status on page 16: Explains the Home page with its summary of the system status.
- Chapter 3: Managing the System Configuration on page 18: Explains how to configure and upgrade the software version and the system.
- Chapter 4: Managing Network Interfaces on page 30: Allows configuration of the Ethernet and wireless interfaces.
- Chapter 5: Viewing Associated Stations on page 44: Lists the associated stations and their configuration into VLANs.
- Chapter 6: Managing System and Station Security on page 52: Explains how to configure new users, passwords, SNMP and HTTP configuration; contains detailed description of SSIDs and VLANs and the relationship between them.
- Chapter 7: Viewing Events on page 80: Explains how to view and configure the system event logs.
- Chapter 8: Upgrading the System Software on page 86: Provides detailed instructions for upgrading the system software version.
- Chapter 9: Appendix: Quick Start Guide to Wavion WS410 on page 90: Intended for first time users of the WS410; contains recommended defaults for first time acquaintance with the system.
- Chapter 10: Appendix: Troubleshooting on page 102: Provides tips on dealing with possible questions you may have in working with the WS410.

Contents

Chapter 1 **USING WS410 WEB-BASED MANAGEMENT INTERFACE .10**

Navigating through the WS410 10
Modifying Data.....12
Saving Data.....13
Using Other Available Options 14

Chapter 2 **VIEWING THE SYSTEM STATUS 16**

Viewing the Home Page.....16

Chapter 3 **MANAGING THE SYSTEM CONFIGURATION 18**

Viewing the System Configuration 18
Setting System Contact Details.....20
Setting the IP Address Configuration 20
Setting the System Management Configuration.....21
Saving Changes.....21
Managing System and Software Configurations 21
Performing Software Upgrades 21
Managing the System Configuration 25
Viewing the System Hardware Components.....28

Chapter 4 **MANAGING NETWORK INTERFACES..... 30**

Viewing the Network Interfaces Summary 30
Managing the Ethernet Interface.....32
Managing the Wireless Interface 34
Setting the Operational Channel 37
Setting the Transmission Power 37
Selecting the Interferer Handling Mode.....38
Saving Changes.....38
Automatic Channel Selection.....39

Chapter 5 **VIEWING ASSOCIATED STATIONS..... 44**

Viewing Stations 44
Viewing Associated Stations.....45
Viewing Specific Stations 46

Chapter 6 **MANAGING SYSTEM AND STATION SECURITY 52**

Viewing the Security Page 52
Viewing the Management Configuration Page 55
Viewing the Authentication Pages 59
Configuring RADIUS Server Parameters: Server Manager Tab 61
Viewing the SSID Pages 62
Viewing and Configuring WEP Security - No VLANs mode 65
Viewing and Configuring WPA Security - No VLANs mode 66
Introducing IEEE 802.11 and WS410 Security Concepts 67
Security Modes: Authentication and Encryption Methods 67
Authentication Combinations 71
Encryption Methods 71
VLAN Introduction and Configuration 72
Tagging VLANs 72
Configuring VLANs 72
Configuring Multiple VLANS per SSID 77
Configuring RADIUS Assigned VLANS 77
Security Modes: Authentication and Encryption Methods 78
Authentication Combinations 79
Encryption Methods 79
SSIDs and VLANs 79

Chapter 7 **VIEWING EVENTS 80**

Viewing the Most Recent Events 80
Viewing the Full Event Log 82
Navigating the Event Log 82
Configuring Event Logs 83

Chapter 8 **UPGRADING THE SYSTEM SOFTWARE 86**

Chapter 9 **APPENDIX: QUICK START GUIDE TO WAVION WS410. 90**

Introduction 90
Connecting the WS410 to a PC 91
Log In 92
Becoming Oriented with the Application 93
Modifying the System Configuration 94
Setting System Contact Details 94
Setting the IP Address Configuration 95
Setting the System Management Configuration 95
Saving Changes 95

Changing the Network Interface Configuration 96
Setting the Operational Channel 96
Setting the Transmission Power 97
Saving Changes 98
Modifying the Security Configuration 98
Renaming the SSID 99
Setting the Security Mode 99
Setting the Authentication Type 99
Setting the Encryption Type 99
Saving Changes 99
Rebooting the System 99
Congratulations! 101

Chapter 10 APPENDIX: TROUBLESHOOTING 102

CHAPTER 1

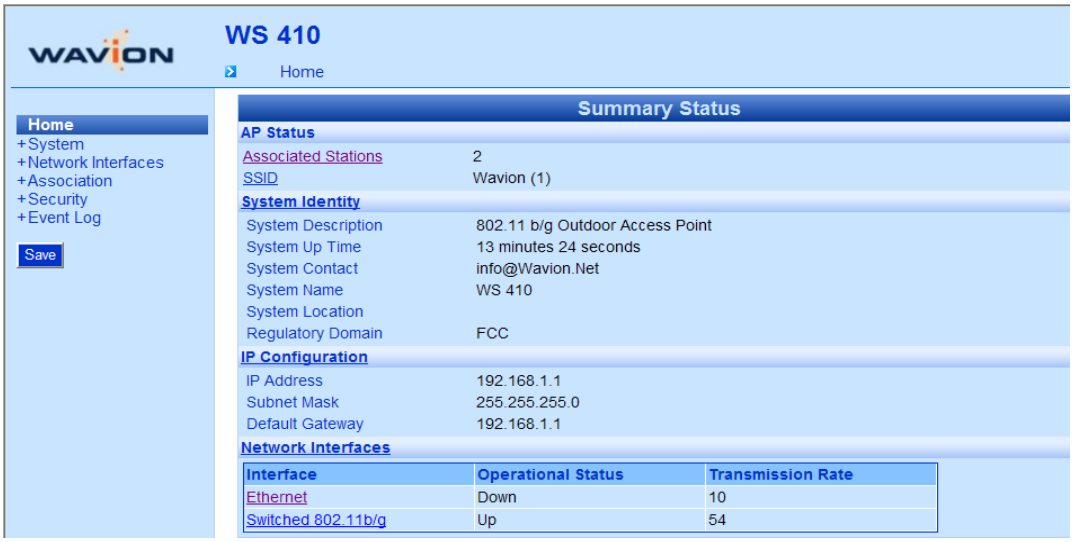
Using the WS410 Web-based Management Interface

This section discusses the Web-based Management interface of the WS410. Covered are page layout, navigation, and modifying data.

Navigating through the WS410

The Web-based Management interface of the WS410 is straightforward. A WS410 page comprises the following main sections: a menu bar, a header, and a main page area.

Figure 1.1. **WS410 Home Page**



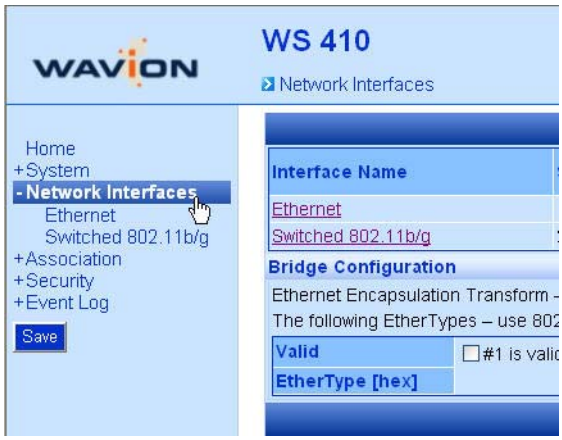
- The menu bar is located on the left side of the screen. This area works like a directory tree. Clicking a menu item causes a different main pages to be displayed, and may cause menu sub-items to appear. You may choose from the menu sub-items to display a specific main page.
- The header contains the system name and user name, and also displays the path to the page. For example, the Home page is reached directly from the menu item Home, so only the word Home is displayed, but when it is necessary to click through additional items on

the menu bar in order to reach a page, all these menu items are listed in order in the header.

- The main page area is specific to the functionality of each particular page.

Initial navigation begins on the left-hand side of the application window. Menu selection items are Home, System, Network Interfaces, Association, Security, and Event Log. Notice that some of these items have a + symbol in front of the name. This signifies that there are additional sub-items under this item.

Figure 1.2. **Navigating the GUI**

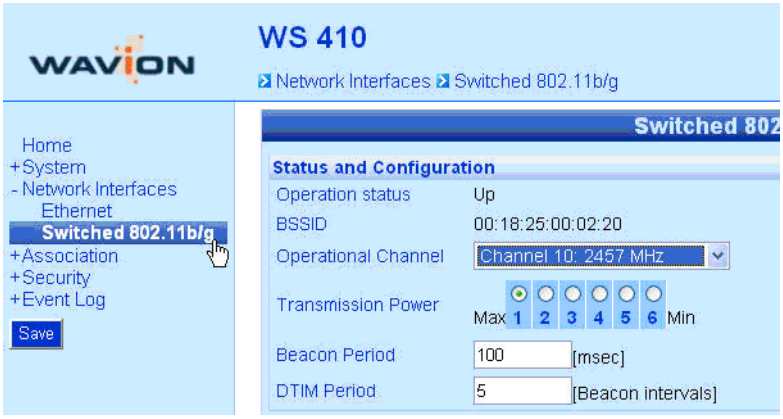


In the figure above, the selection of Network Interfaces is shown. Once the menu item is clicked, the sub-items appear on the menu, and the Network Interfaces page is displayed with the name of the menu item across the top of the main window just below the logo.

There may be more than one way to navigate to a particular page. In the example above, you can either choose Switched 802.11 b/g from the menu sub-item on the left under the Network Interfaces, or, you can select Switched 802.11 b/g from within the Network Interfaces page.

In the example below, the Switched 802.11 b/g is selected from the menu sub-item on the left. The Network Interfaces > Switched 802.11 b/g path shows just under the WS410 logo.

Figure 1.3. **Navigating to a Sub-Item**



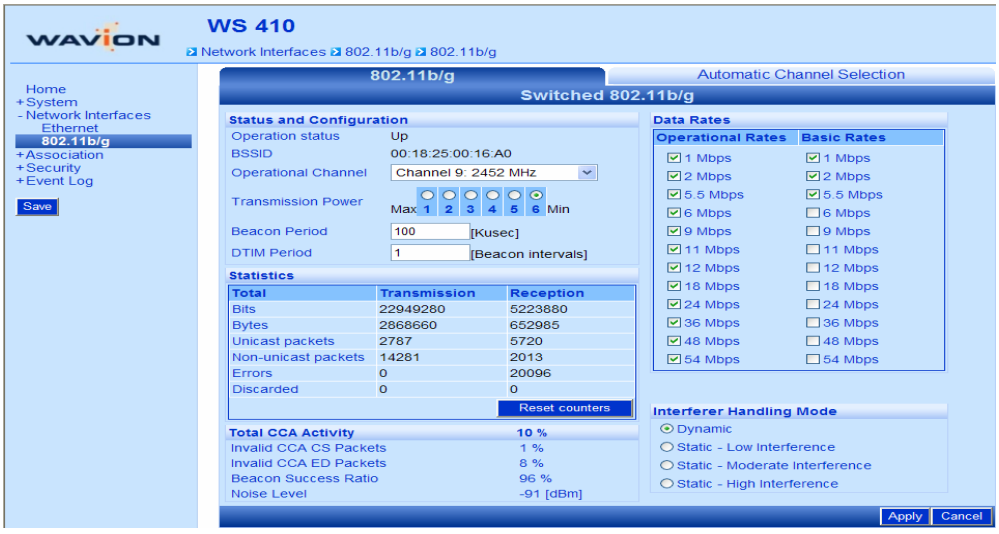
Modifying Data

Modifying data in the WS410 is a simple process and complies with Window's Internet Explorer Web interfaces. There are several types of data-entry fields.

- Text boxes signified by white rectangles allow direct text input
- Dropdown list boxes have a set of options made available by clicking the arrow on the right side of the rectangle
- Radio buttons are clicked to make a selection. Radio buttons are round. They are mutually exclusive; only one of the choices may be selected.
- Check boxes are square. Whereas radio buttons allow only a single selection, many check boxes may be checked at a time.

The example below shows all four possibilities.

Figure 1.4. **Example Showing GUI Elements**



Saving Data

In the WS410, applying data changes to take effect is a process consisting of several steps.

To affect a change in a data field

1. Edit the data in the field or make a selection.
2. Click Apply in the bottom right of the window.

NOTE: You must click Apply before navigating to another page or the changes do not take effect.

When you click Apply, the Web browser shows that the page is busy. Usually, this is shown in the bottom status bar of the browser by an expanding set of green boxes. It is necessary to let this cycle complete before doing anything else.

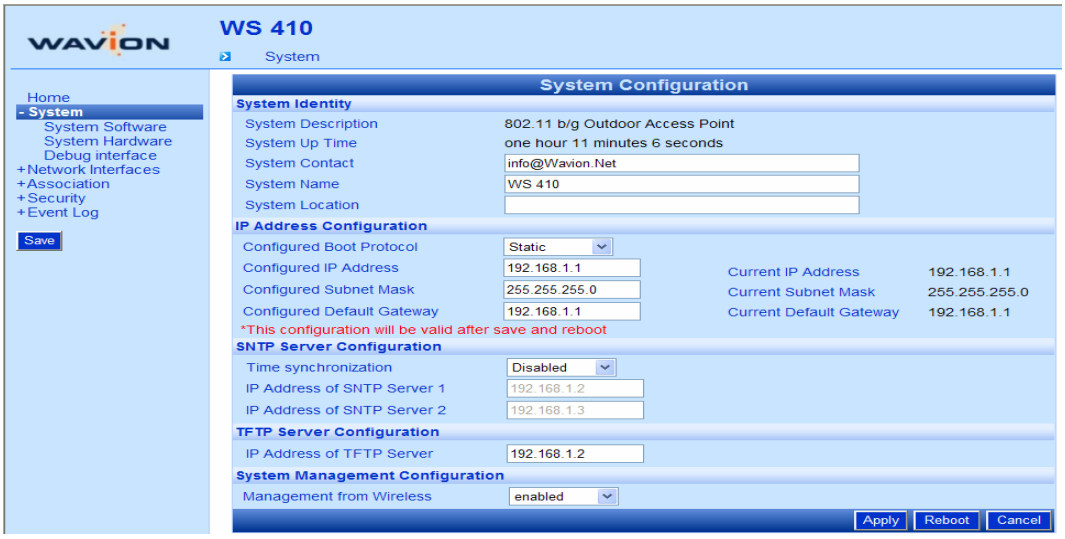
3. In some cases the Apply is sufficient and rebooting is not necessary to make the change effective.

NOTE: If you want the change to be effective following a reboot, you must click Save, otherwise the changes are lost after the reboot.

4. In some cases, a Reboot is necessary to put the changes into effect. Click Save before the Reboot.

Example of a Necessary Save and Reboot

Figure 1.5. **Example Save and Reboot Warning**



In the above example you need to click Save to effect the changes. See an example of the Save button in Figure 1.5 above.

Click Save after making and applying changes.

Again see the indication on the web browser that the request is being processed in the same way as described for the Apply button. It is necessary to let this cycle complete before doing anything else.

NOTE: The red warning message does not go away when Save is pressed. A reboot of the system is still required.

If necessary, reboot the WS410 either by power-cycling the unit, or by clicking Reboot at the bottom of the System window.

Clearing Changes

When making changes, you may decide that you need to return the page to its previous state. This can be done by clicking Cancel.

NOTE: Cancel only works until the point when you click Apply. Once you click Apply, in order to change back, you must re-enter the previous data manually. Alternatively, you can reboot the system without clicking Save.

Using Other Available Options

There are other options available on the WS410 pages. In general, these buttons are specific to the pages where they appear and are described on the relevant pages.

CHAPTER 2

Viewing the System Status

The Home page shows a summary of status data of the system. From within this page, you can quickly link from fields to other related pages for more information.

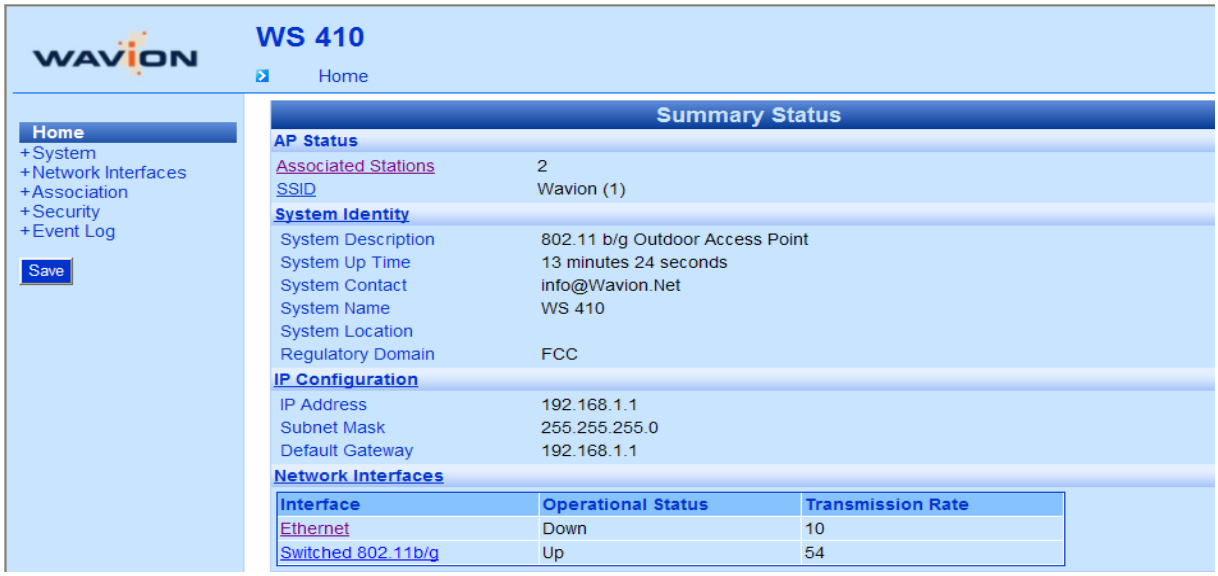
Viewing the Home Page

To view the Home page

- Click Home.

  The Summary Status page is displayed.

Figure 2.1. **Home: Summary Status Page**



The following fields appear on the Summary Status page:

Table 2.1. **Home: Summary Status page**

Field	Description
AP Status	
Associated Stations	Links to Associated Stations page
SSID	Service Set Identifier; links to Editing SSID page

Table 2.1. **Home: Summary Status page**

Field	Description
System Identity	Links to System Configuration page
System Description	Description of the device as written in MIB-II SysDescr OID
System Up Time	Total time since system was switched on or last re-initialized
System Contact	Administratively-assigned email address of system operator
System Name	Administratively-assigned name for this managed node; the node's fully-qualified domain name.
System Location	Administratively-assigned physical location of this node (e.g.,`telephone closet, 3rd floor')
IP Configuration	Links to System Configuration page
IP Address	The current IP address of the unit
Subnet Mask	The current subnet mask used to establish the broadcast domain.
Default Gateway	The current IP address of the default gateway.
Network Interfaces	
Network Interfaces	Links to the page for that interface • Ethernet • Switched 802.11 b/g
Operational Status	Up/down
Transmission Rate	Maximum transmission rate on the interface in Mbps

CHAPTER 3

Managing the System Configuration

The System Configuration page displays system address and IP information. The other system pages allow updating of the software version and system configuration, and a view of the system components.

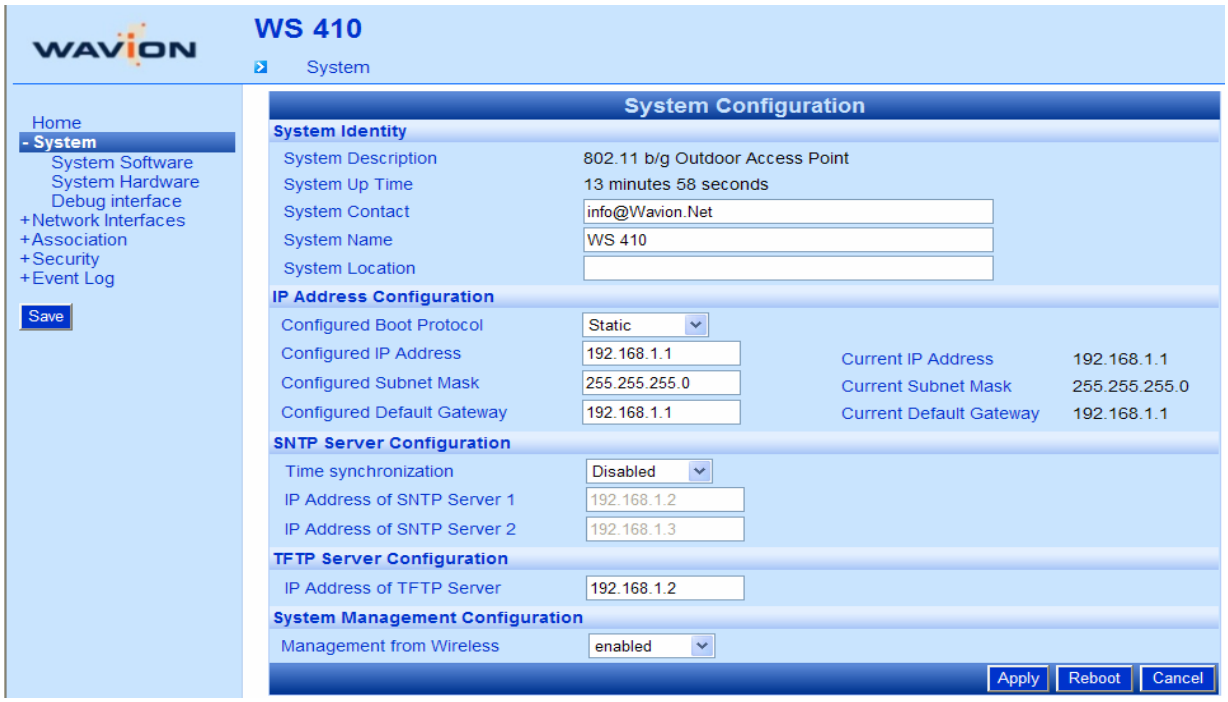
Viewing the System Configuration

To view the System Configuration page

- Click the System menu item.

  The System Configuration page displays.

Figure 3.1. **System Configuration Page**



The following fields appear on the System Configuration page:

Table 3.1. **System Configuration page**

Field	Description
System Identity	
System Description	Description of the device as written in MIB-II SysDescr OID
System Up Time	Total time since system was switched on or last re-initialized
System Contact	Email address of system operator
System Name	Administratively-assigned name for this managed node; the node's fully-qualified domain name.
System Location	Physical location of this node (e.g.,`telephone closet, 3rd floor')
Current IP Configuration	
Current IP Address	IP address of the unit
Current Subnet Mask	Broadcast domain for subnetwork
Current Default Gateway	The IP address of the default Gateway. This address is necessary to contact the WS410 from a remote server.
Configured IP Configuration	
Configured Boot Protocol	• Select DHCP for automatic assignment of IP address from a DHCP server • Select Static to configure IP address manually
Configured IP Address	192.168.1.1 is the default unit’s IP address
Configured Subnet Mask	255.255.255.0 is the default subnet mask
Configured Default Gateway	Default Gateway to be used if forwarding IP address is not in the current subnetwork. Default is blank. This address is necessary to contact the WS410 from a remote server.
Configure TFTP Server	
IP Address of TFTP Server	The IP address of the default TFTP server; can be overridden in the Software Upgrade page for a temporary SW download

Table 3.1. **System Configuration page**

Field	Description
System Management Configuration	
Management from Wireless	• Enable -- to allow system management from the Wireless Interface • Disable -- to allow management only from the Ethernet Interface
Options	
Apply	Click to have changes take effect temporarily
Save (on left side of screen)	Click to have changes made on this page remain even after a reboot; some changes also require reboot to take effect
Reboot	Be sure to click Save first if you made changes you wish to persist after reboot. Click Reboot to have all saved changes take effect
Cancel	Click to clear changes made; Cancel only works on changes where neither Save or Apply was clicked

This page contains basic static information on the system, such as contact details, and IP addresses. Several changes are recommended on this page.

Setting System Contact Details

In the System Identity area, in the System Contact field, enter the contact email address of the net owner.

Setting the IP Address Configuration

Change the IP address to allow the full configuration. The Current IP Address Configuration area lists a default IP address; it is possible to perform initial testing with this address, but it is highly recommended to change the IP address.

To change the IP address

In the Configured IP Address Configuration section,

1. For a DHCP obtained address, select DHCP. Following a reboot, the WS410 will automatically obtain and IP address, Subnetwork, and Default Gateway from the DHCP server.
2. To allow entry of a new IP address, select Static from the Configured Boot Protocol dropdown list.
3. In the Configured IP Address field, enter the required IP address.

4. In the Configured Subnet Mask, enter a valid netmask.

NOTE: The system must be rebooted for these changes to take effect.

Setting the System Management Configuration

You can decide to allow system management from the Wireless Interface, or to allow management only from the Ethernet Interface, for security purposes.

To enable or disable system management from the Wireless Interface

In the System Management Configuration area, in the Management from Wireless field, from the dropdown list, select Enabled to allow system management from the wireless interface, or Disabled to restrict system management to the Ethernet Interface.

Saving Changes

NOTE: After making changes on this page, you must click both Apply and Save, or the changes do not remain in effect after the next reboot.

1. Click Apply.
2. Click Save.

Managing System and Software Configurations

You can change both the system startup configuration and upgrade the software version from the system software tabs.

To access the system software tabs

- Click System Software from the menu, as a sub-item of the System menu item.

  The system software tabs display, consisting of the Software Upgrade tab for managing the system software version, and the System Configuration tab for managing the system configuration.

Performing Software Upgrades

The Software Upgrade tab shows details about the current software version, and allows you to set properties required to install a new software version. It is also possible to return to the factory default software, backup the current version of the software, and return to a previously backed up version of the software.

Figure 3.2. **Software Upgrade Tab**

The following fields appear on the Software Upgrade tab:

Table 3.2. **Software Upgrade tab**

Field	Description
Current Version	
SW Version	Current software version in use
Product Parameters Version	Current version of the internal database holding the system's default parameters
Upgrade Properties	See the chapter Upgrading the System Software on page 82 for details on installing a new software version.
Software Upgrade Protocol TFTP HTTP	Software may be upgraded using either TFTP or HTTP protocols
TFTP Server – IP Address...	IP address of the TFTP server, if, for the current downloading, it is not the same as the default TFTP Server. Setting the value here is only relevant for this download, and does not hold across a Reboot. The Default TFTP Server is set in the System Configuration page. See System Configuration Page on page 18.

Table 3.2. **Software Upgrade tab**

Field	Description
Upgrade System Software Path/File (TFTP download)	Path to the .wj file being TFTP downloaded
Upgrade System Software Path/File (HTTP upload)	Path including the .wj file being HTTP downloaded; select path using the Browse button which is activated if HTTP is selected as the upgrade protocol
Options	
Default	Returns the system to the factory default software version, and erases the following details: • Current configuration file • Current IP setting - leaving the system with Default IP: 192.168.1.1 mask: 255.255.255.0 • Current software version. See Returning to the Default Software Version on page 24.
Upgrade	Used to install a new software version. See Upgrading the System Software on page 82.
Backup	Backs up the current version on the unit itself. See Backing Up the Current Software Version on page 24.
Restore	Restores the version that was previously backed up. See Restoring the Last Saved Software Version on page 25.

Returning to the Default Software Version

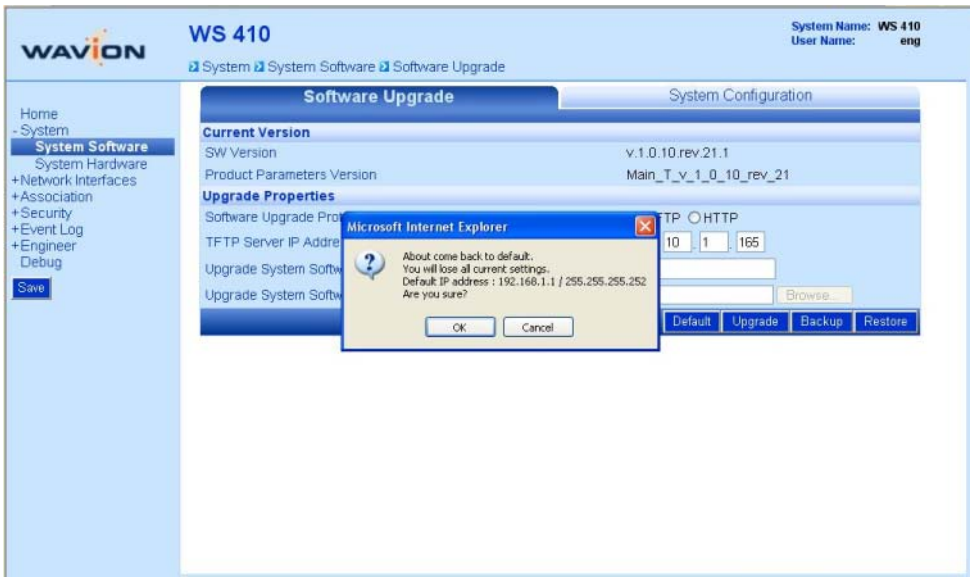
You can reinstall the default software version. If you do this, you lose the current settings and are left with system defaults of IP: 192.168.1.1 and mask: 255.255.255.0

To return to the system default software version

1. Click Default.

   A warning popup displays.

Figure 3.3. **Default Popup**



2. Click OK.

   The system returns to the default software version, and default IP and mask settings.

Upgrading the Software Version

A full description of upgrading the software version is given in Upgrading the System Software section on page 82.

Backing Up the Current Software Version

You can backup the software version currently installed on the system. This can be used before upgrading to a new version with which you do not have experience.

To back up the current version of the software

- Click Backup.

  The current version of the software is saved, and can be restored to the system if necessary.

Restoring the Last Saved Software Version

If you backed up a software version before upgrading to a new one, it is possible to return to the previous version.

To return to a previous system software version

- Click Restore.

  The last backed up version of the system software is restored to the system.

Managing the System Configuration

On the System Configuration tab you can manage current system configuration file name and the configuration management parameters. You can also restore the factory default configuration file, export the current system configuration file, or import a new system configuration file

Figure 3.4. **System Configuration Tab**

The following fields appear on the System Configuration tab:

Table 3.3. **System Configuration tab**

Field	Description
Current Configuration File	
Current Startup Configuration File	File currently used to configure system on startup. This field is also used to export the current configuration file. Right-clicking on the file name alllows you to save the current Startup Configuration File on you local disk. See Exporting the Current Startup Configuration File on page 27
Import New Configuration File	To import a saved configuration file
Import Protocol TFTP/ HTTP	Configuration file can be imported using either TFTP or HTTP protocols
TFTP Server – IP Address...	IP address of the TFTP server, if, for the current downloading, it is not the same as the default TFTP Server. Setting the value here is only relevant for this download, and does not hold across a Reboot. The Default TFTP Server is set in the System Configuration page. See System Configuration Page on page 18.
New Startup Configuration File	Path including the .swcc file being HTTP downloaded; select path using the Browse button which is activated if HTTP is selected as the import protocol
Options	
Factory Defaults	Used to restore the factory default startup configuration. Clicking here erases the configuration file that contains all the changes you made to the unit except the unit's IP address. See Restore to the Factory Default Configuration File on page 27.
Import System Configuration	Used to import a new startup configuration from a previously saved file. See Importing a New System Configuration File on page 27

You have the option of exporting the current startup configuration, importing a new startup configuration or of restoring the factory default configuration file.

Exporting the Current Startup Configuration File

To export the current system configuration

1. Click on the name of the current software configuration.

   A File Download dialog box will appear listing the Name, Type, and From IP address.

2. Click on the Save button of the File Download dialog box.

   A Save As dialog box will appear.

3. Choose the save in folder, create the correct File name, and click on the Save button.

Importing a New System Configuration File

To import a new system configuration

1. Select the import protocol to be used, either TFTP or HTTP.
2. If TFTP is selected, enter the IP address of the TFTP server to be used for the download, if it is not the default server.
3. In the New Startup Configuration File, click Browse and select the file location.
4. Click Import Startup Configuration.

NOTE: Do not click Save.

5. Reboot the system to apply the new configuration.

   The new configuration files take effect.

Restore to the Factory Default Configuration File

To restore the factory default configuration file

1. Click Factory Defaults.

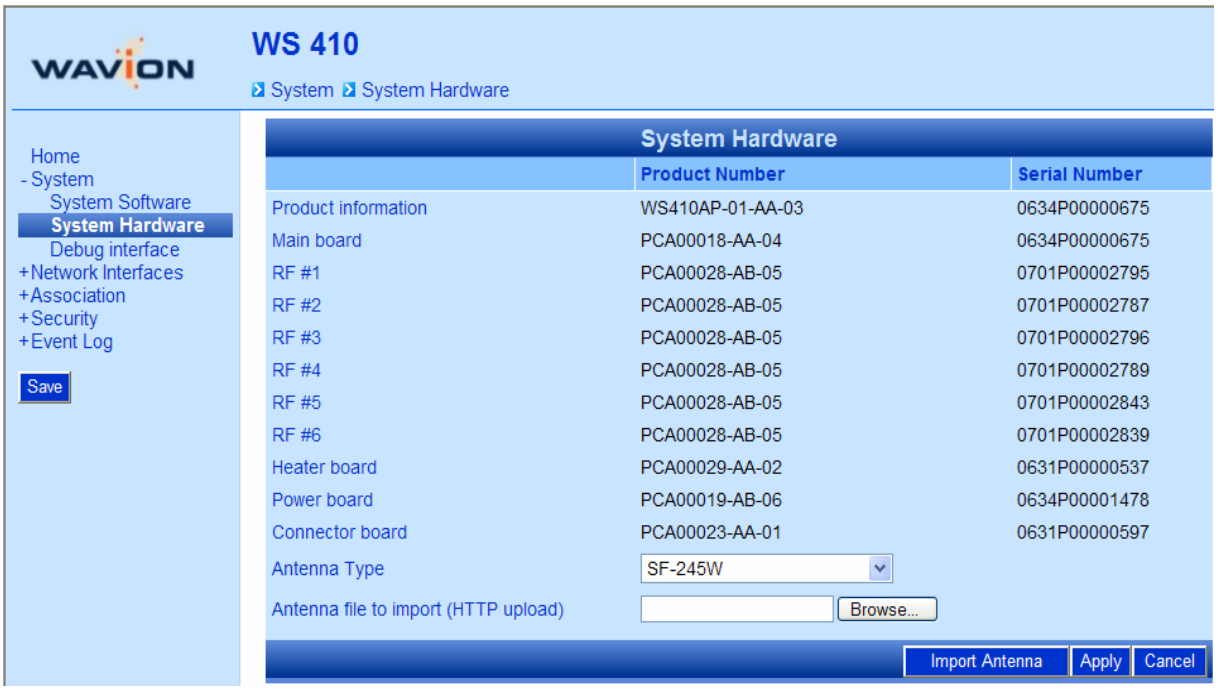
NOTE: This procedure erases the configuration file that contains all the changes you made to the unit except the IP address.
NOTE: Do not click Save.

2. Reboot the system to apply the factory default configuration.

Viewing the System Hardware Components

The System Hardware page lists the components of the system.

Figure 3.5. **System Hardware Page**



The following information is displayed on the System Hardware page for each component.

Table 3.4. **System Hardware page**

Field	Description
Product Number	An internal ID which identifies the components of the system. There are no field replaceable units. This information may be used to identify the hardware components.

Table 3.4. **System Hardware page**

Field	Description
Serial Number	An internal ID which identifies the date of manufacture, production lot, and individual component. There are no field replaceable units. This information along with the product number may be used to identify the specific hardware component.
Antenna Type	The Antenna Type indicates the default antenna type that is installed in the unit. Although WS410 antennas can be detached from the unit, they should be considered as integral part of the WS410. The beamforming capability takes into account the specific attributes of the antennas. Replacement of antenna should never be done without official instructions form Wavion Technical Support person

CHAPTER 4

Managing Network Interfaces

You can view the status of the network interfaces. There is a summary page, and a separate page where each interface can be managed.

Viewing the Network Interfaces Summary

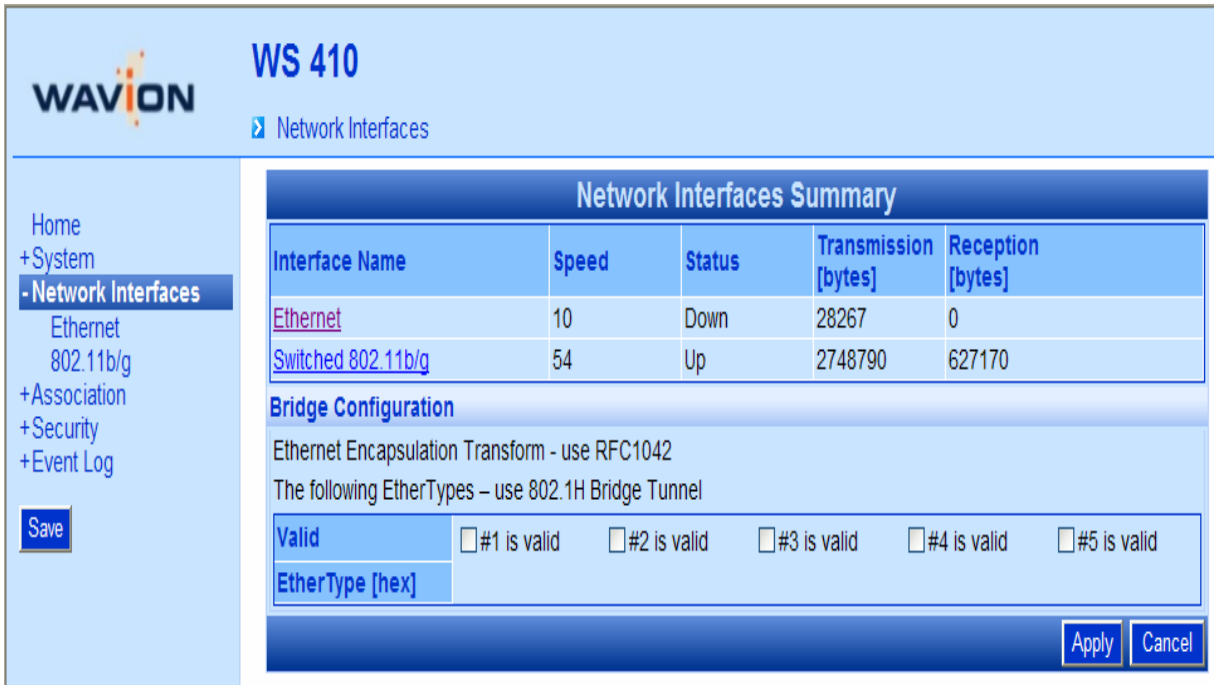
This page displays summary information about the network interfaces.

To view the Network Interfaces Summary

- Click Network Interfaces in the menu.

  The Network Interfaces Summary page displays.

Figure 4.1. **Network Interfaces Summary**



The following fields appear on the Network Interfaces Summary page:

Table 4.1. **Network Interfaces Summary page**

Field	Description
Interface Name	List of network interfaces
Speed	Maximum transmission rate on the interface in Mbps
Status	Indicates whether interface is up or down
Transmission (bytes)	Current total transmission in bytes through the interface
Reception (bytes)	Current total reception in bytes through the interface
Bridge Configuration	For each EtherType that is valid in this table, the 802.1H bridge tunnel encapsulation format is used. Otherwise, RFC1042 applies.
Options	
Apply	Click to have your changes take effect temporarily
Save	Click to have your changes remain in effect after a reboot
Cancel	Click to clear your changes; this is only possible if Apply or Save were not clicked

You can click Ethernet or Switched 802.11b/g on either the page or the menu bar to view the Ethernet or Wireless Interface pages.

Managing the Ethernet Interface

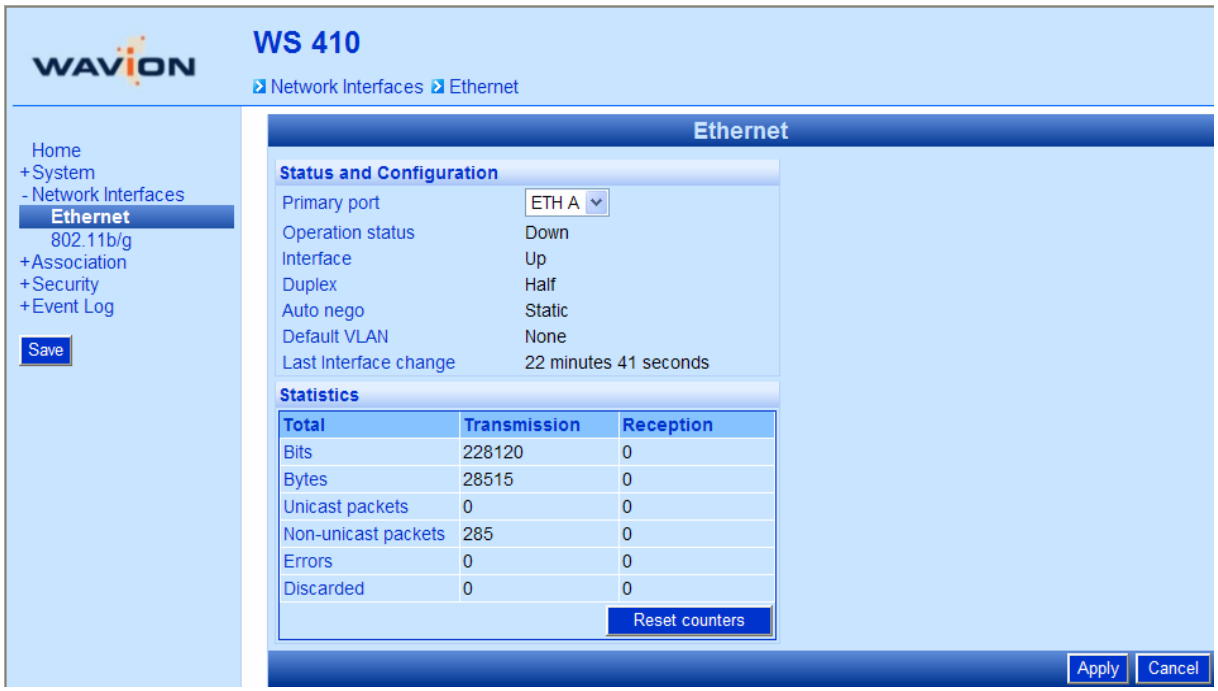
The Ethernet page displays status and configuration parameters, and statistics information for the Ethernet interface.

To view the Ethernet interface parameters and statistics.

- Click Ethernet either from the Network Interfaces Summary or as a sub-item of the Network Interfaces menu item.

  The Ethernet page displays.

Figure 4.2. **Ethernet Page**



The following fields appear on the Ethernet page:

Table 4.2. **Ethernet page**

Field	Description
Status and Configuration	
Primary Port	In case both Ethernet ports are connected, define here which is the primary port through which traffic passes. Selecting an alternate port will not effect the status or statistics.
Operation Status	Up/Down
Interface	Up/Down

Table 4.2. **Ethernet page**

Field	Description
Duplex	Indicates whether transmission through the interface is full duplex or half duplex
Auto Nego	If True, the link is set to auto-negotiation of the transmission rate, if not, the rate is statically set to a specific rate (10 or 100 Mbps)
Default VLAN	Default VLAN of this interface, when working in VLAN mode
Last Interface Change	Total time since last interface change
Statistics	Total amount in Transmission and Reception of the following parameters
Bits	The total number of bits transmitted/ received.
Bytes	The total number of bytes transmitted/ received.
Unicast Packets	The total number of Unicast packets transmitted/received.
Non-Unicast Packets	The total number of Non-Unicast packets transmitted/received.
Errors	The total number of errors that occurred during transmission/reception.
Discarded	The total number of packets that were discarded during transmission/reception.
Options	
Apply	Click to have your changes take effect temporarily
Save	Click to have your changes remain in effect after a reboot
Cancel	Click to clear your changes; this is only possible if Apply or Save were not clicked

Managing the Wireless Interface

The Wireless Interface page displays Status and Configuration details (modifiable), Statistics, Data Rates of the switched 802.11b/g interface, and ACS (Automatic Channel Selection).

To view the Wireless interface parameters and statistics.

- Click Switched 802.11b/g either from the Network Interfaces Summary or as a sub-item of the Network Interfaces menu item.

  The Switched 802.11b/g page displays.

Figure 4.3. **Switched 802.11 b/g Page**

The following fields appear on the Switched 802.11 b/g page:

Table 4.3. **Switched 802.11 b/g page**

Field	Description
Status and Configuration	
Operational Status	Up/Down
BSSID	Identifier MAC address of the AP
Operational Channel	The wireless channel used by the unit. See Setting the Operational Channel section on page 38.
Transmission Power	Should be set to maximum for most applications. Each step towards minimum lessens the transmission power by 3 dB.

Table 4.3. **Switched 802.11 b/g page**

Field	Description
Beacon Period (Kusec)	Amount of time between beacons in kilomicroseconds. One Kusec equals 1,024 microseconds, which is close to 1 millisecond.
DTIM Period (Beacon intervals)	This setting, always a multiple of the beacon period, determines how often the beacon contains a Delivery Traffic Indication Message (DTIM). A traffic indication map is present in every beacon. The DTIM notifies power-save client devices that a packet is waiting for them. If power save clients are active, the access point buffers any multicast traffics and delivers them immediately after the DTIM beacon. Power-save nodes always wait for the DTIM beacons. The longer the time, the more buffering the access point does, and the longer the multicasts are delayed. If the beacon period is set at 100 (default setting), and the DTM Period is set at 1(default setting), then the device sends a beacon containing a DTIM every 100 Kusec.
Statistics	Total amount in Transmission and Reception of the following parameters
Bits	The number of bits transmitted/received.
Bytes	The number of bytes transmitted/ received.
Unicast Packets	The number of Unicast Packets transmitted/received.
Non-Unicast Packets	The number of Non-Unicast Packets transmitted/received.
Errors	The number of errors that occurred during transmission/reception.
Discarded	he number of discards that occurred during transmission/reception.
Total CCA Activity	The relative amount of time (in Percentage) in which Channel was busy. The CCA (Clear Channel Assessment) is the sum of successfully received packets and invalid reception (false alarm)

Table 4.3. **Switched 802.11 b/g page**

Field	Description
Invalid CCA CS Packets	The relative amount of time (in percentage) wasted by unsuccessful receptions (i.e reception that failed to be modulated correctly).
Invalid CCA EDPackets	The relative amount of time (in percentage) wasted by false energy sensing (i.e. energy was detected but no valid carrier was found).
Beacon Success Ratio	The ratio, in percentage, between the number of beacons that the AP transmitted and the beacons that the AP should have transmitted.A low percentage indicates lost beacons probably due to high activity in the channel (CCA is high) that does not enable transmission.
Noise Level	The level of the system noise power in dBm. Nominal noise level without interference is -97 dBm. Higher values indicate higher noise levels due to interference presence.

Table 4.3. **Switched 802.11 b/g page**

Field	Description
Interferer Handling Mode	Select between Dynamic or Static - Low, Moderate, and High. Each selection requires a Reboot to take effect. See Setting the Operational Channel section on page 38. • **Dynamic Mode:** In this mode, the AP Automatically adapts to the interference condition. Sensitivity is decreased (CS and ED) when high interference level is detected • **Static - Low Interference:** Static configuration (Dynamic Handling is Disabled) with maximal sensitivity configuration (maximal range). To be used in non-interfered environment • **Static - Moderate Interference:** Static configuration with mild degraded sensitivity configuration, for moderate interfered environment condition. • **Static - High Interference:** Static configuration with significant degraded sensitivity configurations, for highly interfered environment.
Rates	
Operational Rate	The Operational Rate Set is the set of all of the PHY rates (modulations) that the AP uses for its regular operation.
Basic Rate	The Basic Rate Set is the set of mandatory PHY rates that the clients must support in order to join this AP's network.
Options	
Apply	Click to have your changes take effect temporarily
Save (from the menu bar)	Click to have your changes remain in effect after a reboot
Cancel	Click to clear your changes; this is only possible if Apply or Save were not clicked

On this page you can configure the wireless interface. There are several recommendations for this page.

Setting the Operational Channel

Operational channels should be set up in such a way that if you have multiple units which are located in the same area, they interfere with each other as little as possible. If you have up to three units, it is recommended to use channels 1, 6, and 11, as that minimizes interference between the channels.

The wireless activity in a channel is an important factor in network performance. Channel activity is indicated by Total CCA Activity; low values indicate low activity in the channel.

NOTE: The Total CCA activity represents all traffic; including that of the WS410. Measurements made to select a channel are best performed when there is limited or no traffic to WS410.

To set the Operational Channel

In the Status and Configuration area, from the dropdown list in the Operational Channel field, select the channel on which the system runs. Default is Channel 6: 2437 MHz.

Setting the Transmission Power

Be sure the Transmission Power is set to the maximum; the radio button in this field should be set on the setting closest to the word Max.

Selecting the Interferer Handling Mode

The default Interferer Handing Mode is Dynamic. This mode adaptively changes the system sensitivity according to the interference conditions in the environment. In some cases, using the static (standard) mode may result in better performance than dynamic due to limitations with tracking the exact interference. Such cases may be:

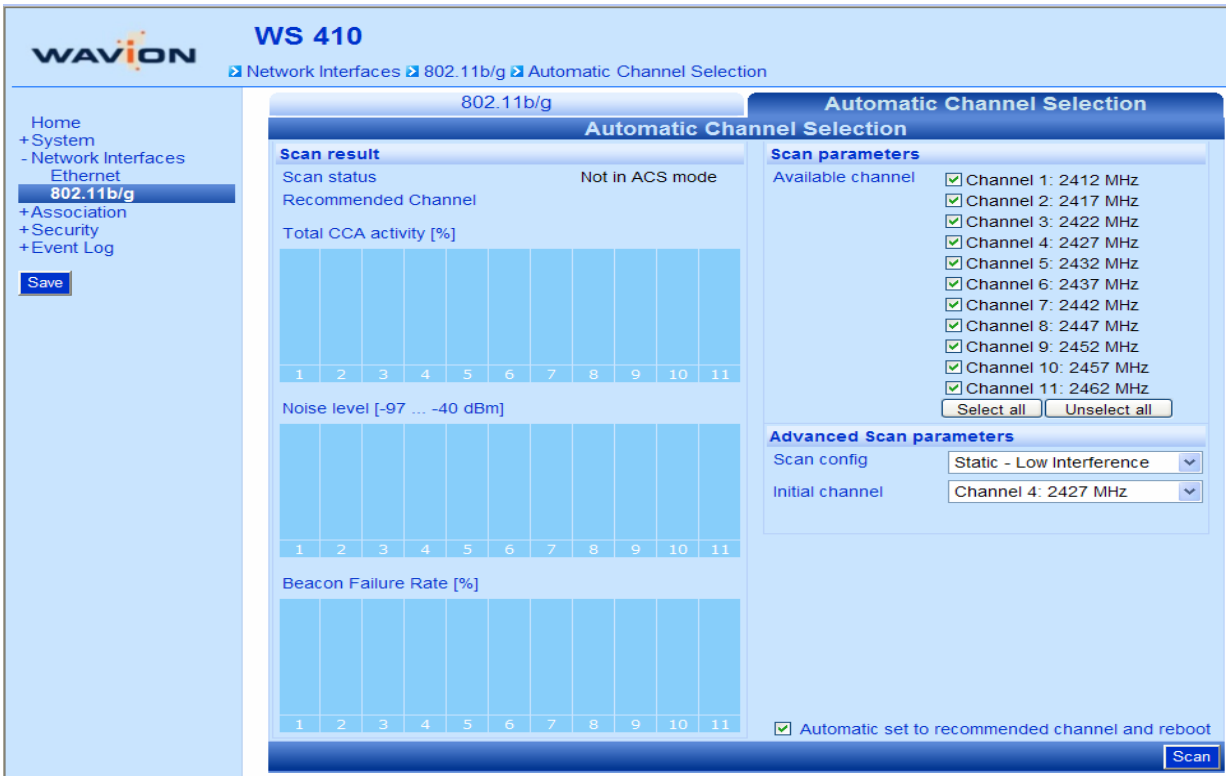
- When the Noise Level measurement indicates the presence of significant interference conditions; that is the noise level is above nominal non-interfered levels and the traffic appears to be low.
- When the maximin range is desired.

Saving Changes

1. Click Apply.
2. Click Save.

The Automatic Channel Selection page displays.

Figure 4.4. **Automatic Channel Selection Page**



General Description:

The Automatic Channel Selection (ACS) is a tool for automatic scanning the frequency channels, and selecting the best channel based on the activity and the interference level of each channel. It is useful for both standalone deployment and in assisting tool for multi-AP deployment.

The ACS scan the selected channels list, display the scanned results to the user, recommend the best channel for operation and re-start the system in this channel.

The scanning activation and results retrieval are available by SNMP to enable centralized operation of the channel scanning and selection.

Note: During scan, clients can not associate to the AP.

Figure 4.5. **Automatic Channel Selection page during Operational Mode**

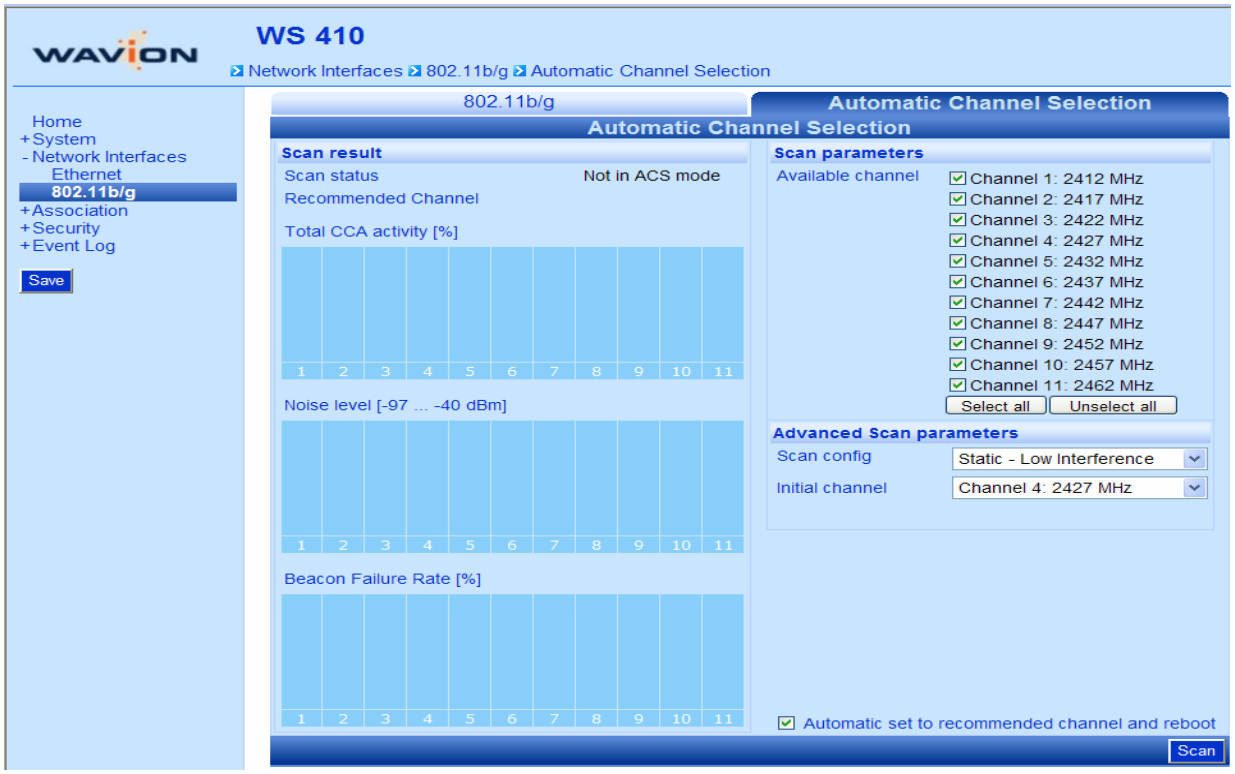
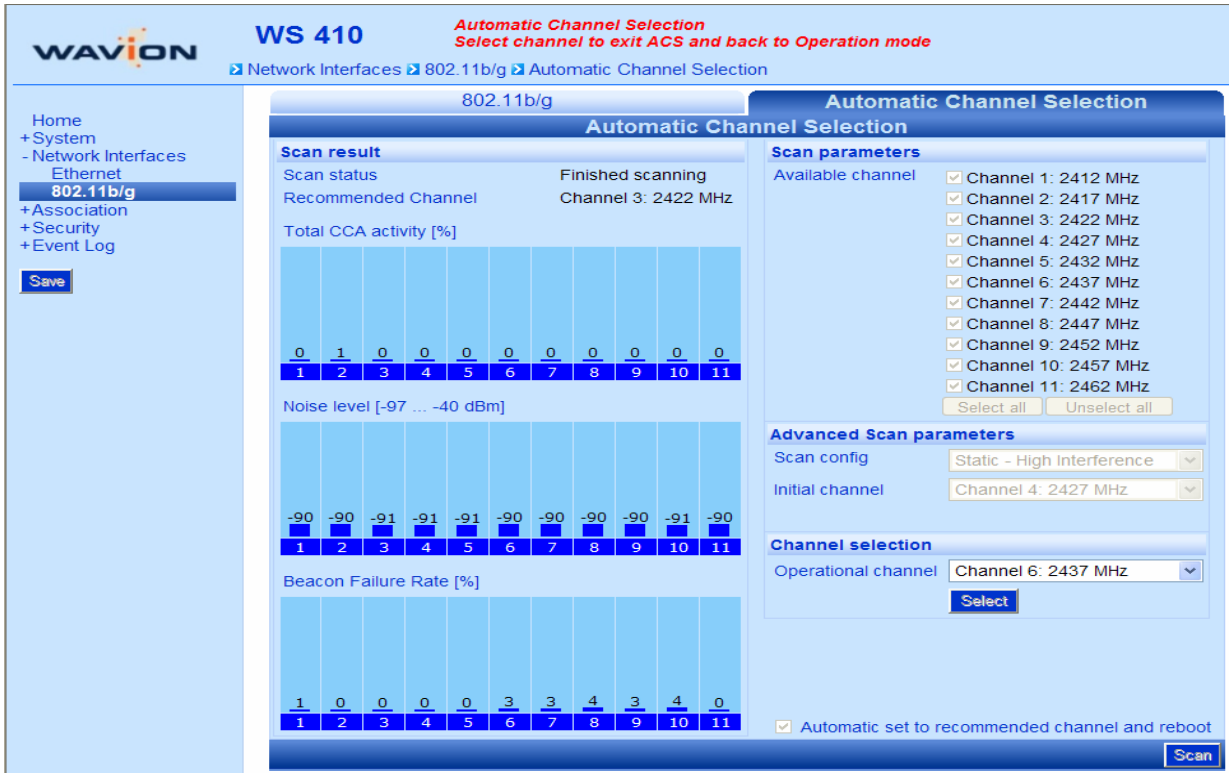


Figure 4.6. **Automatic Channel Selection page after scanning**



How to initiate scan:

Pressing scan button in the ACS page will initiate the scan process. During the process, the system will reboot to Scan Mode, perform the scan and afterwards, reboot back to Operational Mode to the best channel.

During scan mode the system will not be operation, i.e client will not be able to associate, although beacons will continue to be transmitted.

By disabling “Automatic set to recommended channel and reboot” option, the system will not set the recommended channel and will not return to Operational Mode. This enables multiple scanning with the ability to change scanning parameters such as scan, sensitivity, and channel list.

Pay attention that if the “Automatic set to recommended channel and reboot” check box will not be set, the system will remain not operational until the user will manually return to operational mode. During the time the system is not in operation mode, a warning text written in red in the top of the page will indicate this.

How to return to Operational Mode:

If “Automatic set to recommended channel and reboot” check box is set (default configuration), the system will automatically return to operational mode with the selected channel after the scanning.

During any time in which the system is not in operational mode, selecting channel from “Operational channel” list-box and pressing reboot will return the system to operational mode with the selected channel.

The following fields appear in the Automatic Channel Selection page:

Table 4.4. **Automatic Channel Selection page**

Field	Description
Scan Parameters	
Available channel	The list of channel to be scan. Subset of the operational channels can be selected for scanning acceleration or if the user wishes to avoid using some channel. Scanning single channel takes ~10 seconds.
Advance scan parameters	Configuration of the scanning

Table 4.4. **Automatic Channel Selection page**

Field	Description
Scan Configuration	The scan sensitivity. the values can be: • **Static Low Interference:** Highest scan sensitivity • **Static Moderate Interference** • **Static High Interference:** Lowest scan sensitivity The **default** is Static Low Interference. Using lower sensitivity scan will not monitor the weak interference and show only the high power activity.
Initial channel	The channel in which the system perform the calibration before scanning. Scan results are more accurate if initial channel has low interference level.
Automatic set to recommended channel and reboot	• Check Box = The system will reboot to the recommended channel after scanning. • Un-Check Box = The system will scan and display the recommended channel but will stay in scan mode (for further scanning or for manual selection of desired channel)
Scan results	Results of the scanning
Scan Status	Status of the system mode. • Not in ACS mode - is shown during operational mode • Scanning - is shown during scan • Finished scanning - is shown after scanning if the “Automatic set to recommended channel and reboot is not set
Recommended channel	The best channel that was chosen based on scan results. It selects the best channel from channels selected in the “available channel” list. the recommended channel incorporates both noise level and channel activity in the selection.

Table 4.4. **Automatic Channel Selection page**

Field	Description
Total CCA activity	Total activity in the selected channel in percentage
Noise level	Level of the noise as measured by the AP
Beacon failure rate	Percentage of the beacons that the system failed to transmit
Channel Selection	Selection channel for returning to operational mode. These fields appear only in non-operational mode
Operational channel	The channel in which the system will operate when returning to operational mode.
Select	Button for setting the selected channel, saving it, and returning to operational mode. A warning box will appear for acknowledgement after pressing this button.

CHAPTER 5

Viewing Associated Stations

The Association menu item allows you to view parameters of associated stations to the system.

Viewing Stations

To view a summary of associated stations

- Click the Association menu item.

The following summary chart appears if there are associated stations in the system.

Figure 5.1. **Association Statistics**

The following fields appear on the Association Statistics page:

Table 5.1. **Associated Stations page**

Field	Description
Associated Stations	links to list of Associated Stations
Number	Number of associated stations

Viewing Associated Stations

You can view a summary list of associated stations and their parameters

To view a summary list of stations and parameters

1. Click Association on the menu.
2. Click Associated Stations on the menu bar or on the summary screen

   The Associated Stations page is displayed.

Figure 5.2. **Associated Stations Page**

The following fields appear on the Associated Stations page:

Table 5.2. **Associated Stations of VLANS page**

Field	Description
Title	
Station's MAC Address	Physical or MAC (Media Access Control) address of the associated station
Power Save State	Value of Doze in this field indicates that the associated station is in power save mode
WME s[Mbps]upport	No
Oper. Rate [Mbps]	PHY Rate (modulation) at which the associated station currently communicates
VLAN	VLAN name to which the station is bound (if applicable)
Tx[Bytes]	Number of bytes transmitted by AP to the station
Rx[Bytes]	Number of bytes received by the AP from the station

Table 5.2. **Associated Stations of VLANS page**

Field	Description
RSSI[dBm]	The Received Signal Strength Indicator power received by the AP from the associated station.
State	State of which the station is connected

Viewing Specific Stations

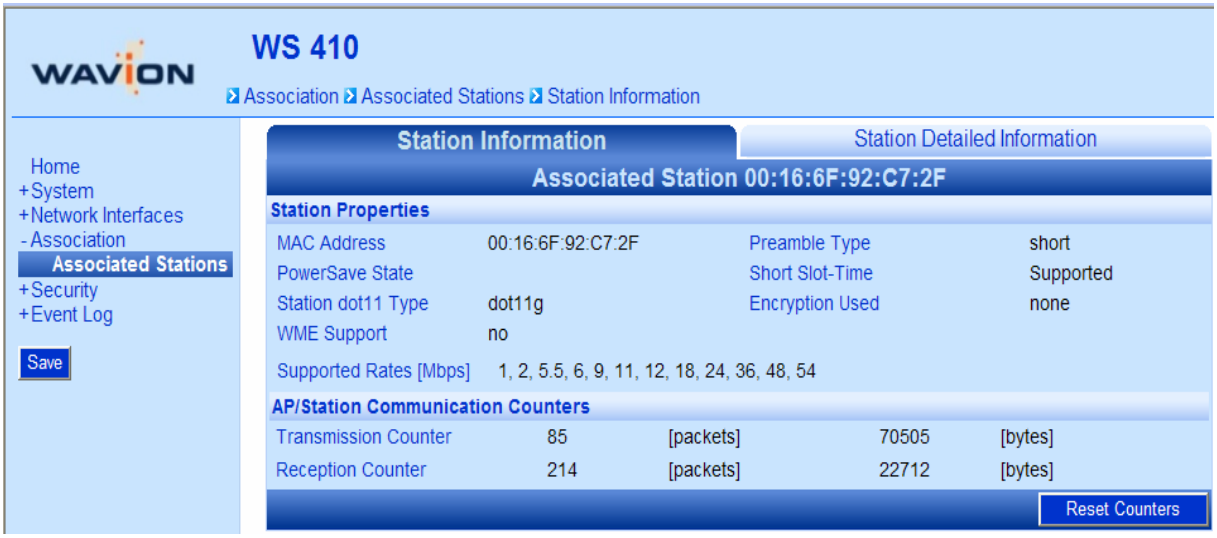
You can view detailed information about a specific station.

To view detailed information about a specific station

- In the Associated Stations summary page, click the Stations's MAC Address for the specific station.

  The Station Information tab is displayed for the associated station.

Figure 5.3. **Station Information tab**



The following information is displayed under the Station Information tab.:

Table 5.3. **Station Information tab**

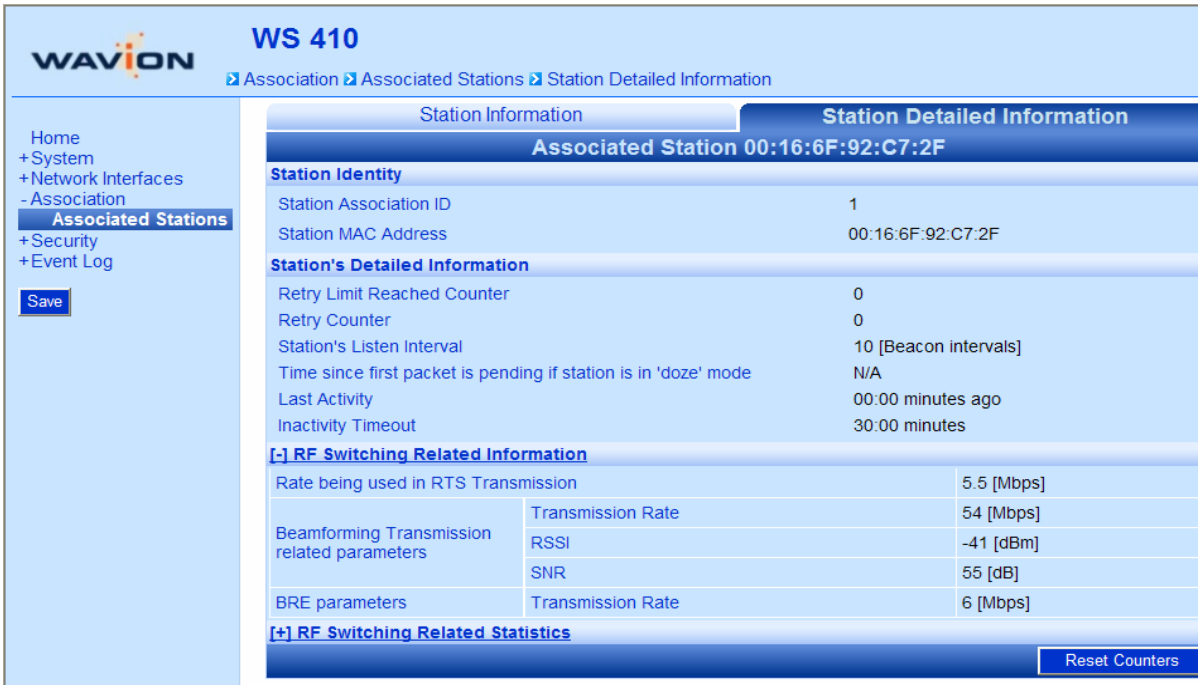
Field	Description
Station Properties	
MAC Address	Physical or MAC (Media Access Control) address of the associated station
Power Save State	Value of Doze in this field indicates that the associated station is in power save mode

Table 5.3. **Station Information tab**

Field	Description
Station dot11 Type	Indicates whether the station is 802.11g or 802.11b.
WME Support	No
Supported Rates [Mbps]	PHY Rates (modulation) at which the associated station can communicate
Preamble Type	The preamble types may be Short or Long
Short Slot - Time	This field indicates whether the client supports Short Slot Time
Encryption Used	The type of encryption used to communicate with this client.
AP/Station Communication Counters	
Transmission Counter	Total transmission to the station shown in number of packets and number of bytes
Reception Counter	Total reception from the station shown in number of packets and number of bytes

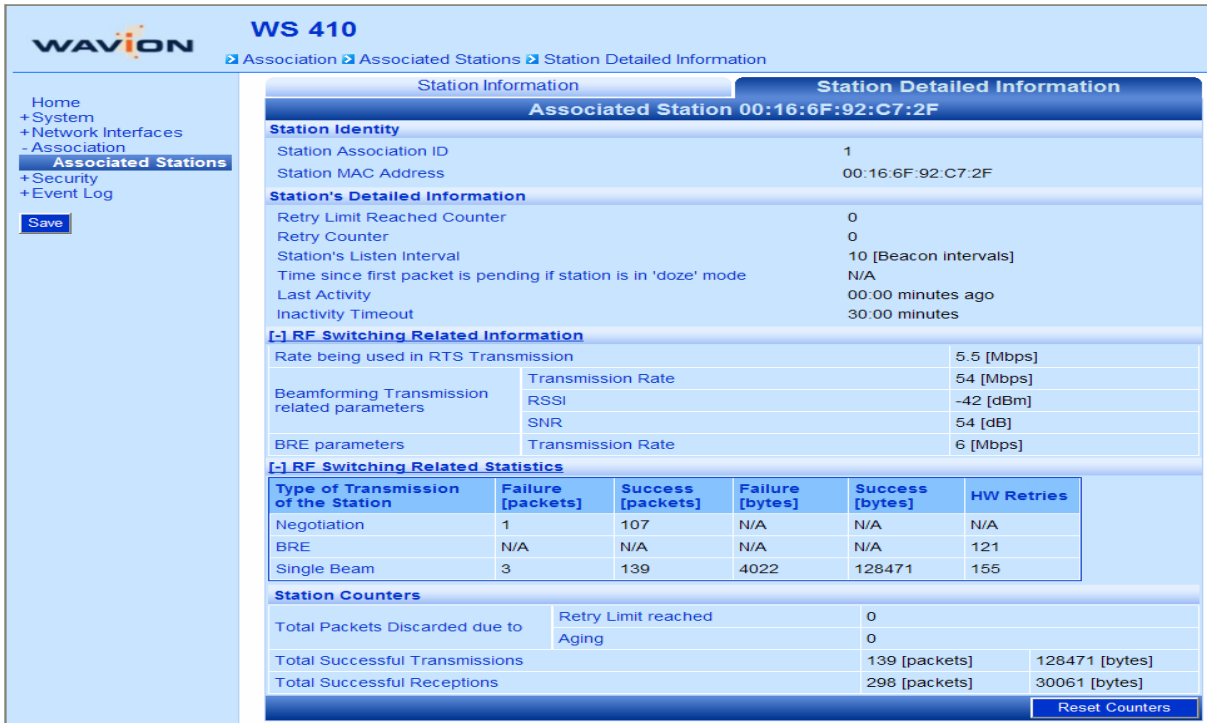
You can select the Station Detailed Information tab to view more details about the same station. This page is long, having a plus sign to click for more information.The page is shown here in two separate figures.

Figure 5.4. **Station Detailed Information tab part 1**



In the above screen, the top of the tab is shown, with RF Switching Related Information plus sign is clicked. In the figure below, the RF Switching Relating Statistics plus sign is clicked and the bottom of the page is shown.

Figure 5.5. **Station Detailed Information tab part 2**


WAVION
WS 410
Association Associated Stations Station Detailed Information
Home
+System
+Network Interfaces
-Association
Associated Stations
+Security
+Event Log
Save
Station Information
Station Detailed Information
Associated Station 00:16:6F:92:C7:2F
Station Identity
Station Association ID 1
Station MAC Address 00:16:6F:92:C7:2F
Station's Detailed Information
Retry Limit Reached Counter 0
Retry Counter 0
Station's Listen Interval 10 [Beacon intervals]
Time since first packet is pending if station is in 'doze' mode N/A
Last Activity 00:00 minutes ago
Inactivity Timeout 30:00 minutes
[-] RF Switching Related Information
Rate being used in RTS Transmission 5.5 [Mbps]
Beamforming Transmission related parameters
Transmission Rate 54 [Mbps]
RSSI -42 [dBm]
SNR 54 [dB]
BRE parameters Transmission Rate 6 [Mbps]
[-] RF Switching Related Statistics
Type of Transmission of the Station | Failure [packets] | Success [packets] | Failure [bytes] | Success [bytes] | HW Retries
Negotiation | 1 | 107 | N/A | N/A | N/A
BRE | N/A | N/A | N/A | N/A | 121
Single Beam | 3 | 139 | 4022 | 128471 | 155
Station Counters
Total Packets Discarded due to Retry Limit reached 0
Aging 0
Total Successful Transmissions 139 [packets] 128471 [bytes]
Total Successful Receptions 298 [packets] 30061 [bytes]
Reset Counters

The following information is displayed in the Station Detailed Information tab.

Table 5.4. **Station Detailed Information tab**

Field	Description
Station Identity	
Station Association ID	The Association ID (AID) that the client got when its assocation to the AP was completed.
Station MAC Address	Physical or MAC (Media Access Control) address of the associated station.
Station's Detailed Information	
Retry Limit Reached Counter	This counter increments every time the Retry Counter (below) reaches its limit (64).
Retry Counter	A counter of the retransmissions to this associated station.
Station's Listen Interval	The listen interval of the client specified during association to the AP.

Table 5.4. **Station Detailed Information tab**

Field	Description
Time since first packet is pending if station is in Doze mode	If station is in Power Save mode, the amount of time for which the first packet received is waiting to be delivered
Last Activity	Number of minutes since the station was last active.
Inactivity Timeout	If a station is not active for this number of minutes, the AP will de-authenticate it due to inactivity.
RF Switching Related Information	Click + sign to display this information/ click - sign to hide
Rate being used in RTS Transmission	The PHY rate (modulation) that the AP uses for transmission of Self-CTS and RTS transmissions to the client.
Beamforming Transmission related parameters:	
Transmission Rate[Mbps]	The PHY rate (modulation) that is used in Beamforming transmission to this client.
RSSI[dBm]	RSSI -- Received Signal Strength Indication as the client is received by the AP.
SNR[dB]	SNR -- Signal to Noise Ratio (dB) as the client is received by the AP.
BRE parameters: Transmission Rate	BRE - Broadcast Range Enhancement. The PHY rate (modulation) in which the AP broadcasts are being transmitted.
RF Switching Related Statistics	Click + sign to display this information/ click - sign to hide
Type of Transmission of the Station	• Negotiation • BRE • Single beam (beamforming) For each of the AP's transmission types to the station, the following transmission statistics are displayed:
Failure (packets)	Number of packets that failed to be transmitted. This number only applies to to Negotiation and Single Beam (beamforming) transmissions and are those which did not receive an ACK response.

Table 5.4. **Station Detailed Information tab**

Field	Description
Success (packets)	Number of packets transmitted successfully. This count is applicable to Negotiation and Single beam (Beamforming) transmissions and are those that received an Acknowledgement (ACK).
Failure [Bytes]	Number of bytes that failed to be transmitted. This is only applicable to single beam (Beamforming) transmissions as they are the only variable length transmissions that receive ACKs.
Success [Bytes]	Number of bytes that were transmitted successfully. This is only applicable to single beam (Beamforming) transmissions as they are the only variable length transmissions that receive ACKs.
HW Retries	Number of hardware retries that were used for the specific transmission type. Negotiation packets are not automatically retried by the hardware, therefore, this count only applies to BRE and Single beam.
Station Counters	
Total Packets Discarded due to	• Retry Limited reached -- Number of undelivered packets that were discarded following maximum number of transmission retries • Aging -- Number of undelivered packets that were discarded because aging-time-out is exceeded
Total Successful Transmissions	• Total successful transmissions delivered to the client measured in packets • Total successful transmissions delivered to the client measured in bytes
Total Successful Receptions	• Total successful transmissions received from the client measured in packets • Total successful transmissions received from the client measured in bytes

CHAPTER 6

Managing System and Station Security

You can manage system users and their passwords, as well as system security parameters. This chapter covers the following main areas:

- Administration in Viewing the Management Configuration Page on page 55
- Authentication in sub-menuViewing the Authentication Pages on page 59
- SSID and VLANs -- this area contains a full description of the concepts of VLANs and SSIDs in the system -- in Introducing IEEE 802.11 and WS410 Security Concepts on page 68

Viewing the Security Page

The Security page displays a summary of the different types of security information: administration, authentication, and SSID/VLAN data. The information on this page varies by the mode VLANs and no VLANs.

To view the Security page

- Click Security in the menu.

  The Security page displays in No VLANs mode.

Figure 6.1. **Security Page / no VLANs mode**

The following fields appear on the Security page:

Table 6.1. **Security Page**

Field	Description
System Mode Selection	
VLAN Mode/ No VLAN Mode	Toggles between VLANs mode and No VLANs mode
Administration	links to the Management Configuration page
User Name	User name of current user
User Type	The security level of the current user: Administrator/Viewer/Superuser
SSID (# of active SSIDs)	The list of active Service Set IDentifiers
SSID name	Identifier of each active SSID
VLAN name	In VLANs mode page only. For each active SSID, there is listed an active VLAN

You can click VLANs Mode to view the Security/VLANs Mode page.

Figure 6.2. **Security / VLANs Mode page**

You can un-check VLANs mode to return to the Security/No VLANs page.

Viewing the Management Configuration Page

The Management Configuration page is used for overall system user and configuration management. You can add new users, change passwords, and update the SNMP and HTTP configurations. Each section is separate, and has its own Apply and Cancel buttons.

To view the Management Configuration page

- Click Administration, either from the Security page, or from the menu bar, as a sub-menu under the Security item.

  The Management Configuration page displays.

Figure 6.3. **Management Configuration Page**

The following fields appear on the Management Configuration page:

Table 6.2. **Management Configuration page**

Field	Description
HTTP/CLI Users	Use to change password or add new users to manage the unit; see below
User Name	When registering a new user, enter user name; user name is case sensitive
User Type	User type is selected when registering a new user Administrator/Viewer
New Password	Use this field to insert new user's password or to change existing password
Confirm Password	When registering a new user, or changing a password, re-enter the above password to verify that the password is correct.
Options	Click buttons in this section with respect to new and current users
Apply	Click to have changes take effect temporarily
Save (on menu bar)	Click to have changes made on this page remain even after a reboot
Cancel	Click to clear changes made; Cancel only works on changes where neither Save or Apply was clicked
SNMP Configuration	
SNMP Enabled	If checkbox is marked, indicates that SNMP is enabled
SNMP Version (V2 or V3)	Lists SNMP version
SNMP Read Community SNMP Write Community	SNMP Read and Write community strings authenticate access to MIB objects and function as embedded passwords
Options	Click buttons in this section with respect to changes made in the SNMP section
Apply	Click to have changes take effect temporarily
Save (on menu bar)	Click to have changes made on this page remain even after a reboot
Cancel	Click to clear changes made; Cancel only works on changes where neither Save or Apply was clicked

Table 6.2. **Management Configuration page**

Field	Description
HTTP Configuration	Use this section to enable secure browsing by creating an SSL certificate See below
Enable Secure Browsing (SSL only)	If the checkbox is marked, it indicates Secure Browsing (SSL) is enabled, and non-secured browsing is disabled.
Create new SSL certificate (using the following identifiers	If the checkbox is marked a new SSL certificate will be created using the following identifiers:
System Name	An administratively-assigned name for this managed node.
Domain Name	An administratively-assigned node's domain name.
Options	Click buttons in this section with respect to changes made in the HTTP Configuration section
Apply	Click to have changes take effect temporarily
Save (on menu bar)	Click to have changes made on this page remain even after a reboot.
Cancel	Click to clear changes made; Cancel only works on changes where neither Save or Apply was clicked

To change a password

1. In the HTTP/CLI Users section, select the user name for which you want to change the password in the username dropdown box.
2. Enter a new password in the New Password field. A password contains at least 6 characters.
3. Re-enter the new password in the Confirm Password field.
4. Click Apply.

   Confirmation pop-up box is displayed.
5. Click OK.
6. Click Save for the password change to remain after a reboot.

To add a new user to the system

1. In the HTTP/CLI Users section, select (new) from the User Name dropdown list.

   A New User field appears.
2. Enter a new user name in the field.
3. Select a user type from the user type dropdown list, either Administrator or Viewer.

4. Enter a password in the Password field. A password must contain at least 6 characters.
5. Re-enter the password in the Confirm Password field.
6. Click Apply.
7. Click Save to retain the new user after a reboot.

To enable secure browsing/create an SSL certificate

1. In the HTTP Configuration section, select Enable Secure Browsing.
2. Select Create new SSL certificate.
3. Enter the system name.
4. Enter the domain name.
5. Click Apply.

   A popup asks if you want to enable only SSL browsing (HTTPS).
6. Click OK.

sub-menuViewing the Authentication Pages

The Authentication pages allow you to configure authentication parameters.

To view the Authentication pages

- Click Authentication, either from the Security page, or from the menu bar, as a sub-menu under the Security item.

  The Authentication pages display. The Authentication pages consist of the Authentication tab and the Server Manager tab.

Figure 6.4. **Authentication Tab**

The following fields appear on the Authentication tab.

Table 6.3. **Authentication tab**

Field	Description
Re-Authentication	
EAP Re-Authentication Interval	When EAP authentication is used, re-authentication of registered clients occurs at this interval
Re-Keying Group Key	

Table 6.3. **Authentication tab**

Field	Description
Re-Keying Method	For WPA SSIDs, the administrator determines if and how often re-keying to broadcast keys occurs. • Disabled – no re-keying • Time Based – re-keying after a certain time • Packet Counter Based – re-keying when group (broadcast) packet counter reaches a certain level (modifiable field)
Timeout (seconds)	After this timeout, re-keying occurs if re-keying method is 'Time Based' (modifiable field)
Packet Threshold	Group broadcast packets' threshold after which re-keying occurs if the method is 'Packet Counter Based'; the value is inserted as multiplication of 1000 packets
Re-Keying on membership termination	Indicates whether a group key re-keying occurs when a client is disassociated from the group.
Options	
Apply	Click to have changes take effect temporarily
Save (from the menu)	Click to have changes made on this page remain even after a reboot.
Cancel	Click to clear changes made; Cancel only works on changes where neither Save or Apply was clicked

Modifiable fields on this page are indicated in the table.

Configuring RADIUS Server Parameters: Server Manager Tab

The Server Manager tab allows you to configure parameters for the RADIUS server.

To view and configure the Radius Server pages

- Click SSID-VLAN, either from the Security page, or from the menu bar, as a sub-menu under the Security item.
- Choose WPA Radius from the Authentication drop down menu to open the Radius Servers configuration.

  Make changes as needed.

Figure 6.5. **Server Manager Tab**

The following fields appear on the Server Manager tab:

Table 6.4. **Server Manager tab**

Field	Description
RADIUS Server IP Address	IP Address of the RADIUS Server. If more than 1 address appears in the list, the following RADIUS Servers are used as backup (only if the previous RADIUS Servers cannot be reached).
Shared Secret	The Shared Secret is a secret that the unit shares with the RADIUS server. This way, both ends know they are "certified".
Options	
Apply	Click to have your changes take effect temporarily
Save (from the menu)	Click to have your changes remain in effect after a reboot
Cancel	Click to clear your changes; this is only possible if Apply or Save were not clicked

You can modify fields on this page.

Viewing the SSID Pages

SSIDs are supported in two modes; Non-VLAN and VLAN. Non-VLAN mode is presented first in this documentation. The reference section on security Introducing IEEE 802.11 and WS410 Security Concepts on page 68 may be helpful in reviewing the SSID pages.

Following the presentation of Non-VLAN SSIDs is that of VLAN, see VLAN Introduction and Configuration on page 70.

To view the SSID pages

- Click SSID, either from the Security page, or from the menu bar, as a sub-menu under the Security item

  The SSID page displays. This page allows management of the security configuration. It is recommended to rename the SSID..

NOTE: The SSID pages are displayed differently depending upon their VLAN mode (These concepts are explained in the following sections). In the factory default, No-VLAN mode, the Broadcast SSID (BSSID) will be displayed. In VLAN mode, multiple SSIDs are enabled. Clicking SSID will display a table of SSIDs from which you may select the single SSID of interest.

The following description will apply to the non-VLAN mode

NOTE: The SSID is case sensitive and shorter than 32 characters.

Figure 6.6. **Editing SSID -- No VLANs mode**

The following fields appear on the Editing SSID page. For more information about Security Configurations, see also on page 76

Table 6.5. **Editing SSID page**

Field	Description
Security Configuration	
Rename SSID	Set new name for the SSID; the SSID is case-sensitive, and less than 32 characters
Authentication	Open System Shared Key Open System + Shared Key WPA PSK WPA Radius WPA PSK + Radius
Encryption	None WEP/40 WEP/104 TKIP TKIP+WEP/40 TKIP+WEP/104
Exclude Unencrypted	When this checkbox is marked, the AP excludes incoming packets that are unencrypted.

Table 6.5. **Editing SSID page**

Field	Description
Options	
Apply	Click to have your changes take effect temporarily
Save (from the menu)	Click to have your changes remain in effect after a reboot
Cancel	Click to clear your changes; this is only possible if Apply or Save were not clicked

Viewing and Configuring WEP Security - No VLANs mode

To view the SSID WEP Security - No VLAN mode pages

- Click the WEP radio button in the Editing SSID page (See figure below).
- Select from the Authentication choices either Open or Shared Key. Shared Key is recommended.
- Select either WEP/40 or WEP/104 from the Encryption choice.
- Enter up to 4 WEP keys. Their length is dependent upon the choice selected in the step above; WEP/40 is 10 hex characters and WPE/104 is 26 characters.

Figure 6.7. **Editing SSID / No VLANs Mode -- WEP Security mode**

Table 6.6.

Field	Description
Security Keys	This section dsplays when a security mode is chosen
WEP Key #	The key # (1-4) indicate the index of the WEP Key.
WEP Key #	The Key value is the hexadecimal value of the WEP key as stored in HW. For the WEP/40 this key holds 10 hexadecimal characters, for WEP/104 this key holds 26 hexadecimal characters.
Options	
Apply	Click to have changes take effect temporarily
Save (from the Menu)	Click to have changes remain in effect after a reboot
Cancel	Click to clear your changes;this is only possible if Apply or Save were not clicked

Viewing and Configuring WPA Security - No VLANs mode

To view the SSID WPA Security - No VLAN mode pages

- Click on the SSID-VLAN Menu (See figure below).
- From the Authentication drop down menu, select either WPA PSK, WPA RADIUS or WPA PSK + RADIUS.
- Select either TKIP, TKIP + WEP/40 or TKIP + WEP/104 from the Encryption choice.
- Enter up to 4 WEP keys. Their length is dependent upon the choice selected in the step above; WEP/40 is 10 hex characters and WPE/104 is 26 characters.
- For the Security Keys, select either by Value or by Pass Phrase and enter the appropriate value

Figure 6.8. **Editing SSID / No VLANs Mode -- WPA Security Mode**

Introducing IEEE 802.11 and WS410 Security Concepts

IEEE 802.11 security is supported by the WS410 in two modes; Non-VLAN and VLAN.

In Non-VLAN mode, all associated stations share the same wireless media and therefore have a single broadcast domain. When a client associates to the SSID, security credentials are checked and encryption keys (both unicast and broadcast keys) are assigned. All security modes are supported through the SSID; see Security Modes: Authentication and Encryption Methods

In VLAN mode, the shared wireless media is divided into various groups or Virtual LANs. All members of a single group can communicate with members of the same group, but cannot communicate with members of any other group; they exist in different broadcast domains. Each group has independent security credentials and encryption keys. As in the Non-VLAN mode, the SSID handles the security used in both Unicast and Broadcast transmissions according to the keys maintained in the VLAN. This is a straightforward pairing of information when there is a single VLAN per SSID. In the event that multiple VLANs (which can only be assigned by a RADIUS server) are on a single SSID, the SSID uses the appropriate VLAN key when communicating to a particular associated station. This insures that both unicast and broadcast transmissions are VLAN specific. As in the Non-VLAN mode, all authentication and encryption methods are supported.

Security Modes: Authentication and Encryption Methods

The following are the different combinations of security modes.

Security Mode	Authentication Mode	Encryption Mode
None	Open system	None
WEP	• Open system • Shared key • Open system + Shared key	• WEP/40 • WEP/104
WPA	• PSK (Pre-shared key) • Radius • PSK + Radius	• TKIP • TKIP+WEP/40 • TKIP+WEP/104

Authentication Combinations

WS410 allows authentication of various types and in various combinations.

- The basic 802.11 authentications are Open (none) and Shared Key. In Shared Key Authentication, the WEP key is used as the shared key.

  If the SSID is configured to Open + Shared Key, this means that both types of clients can associate to the AP. This can be useful when the IT has another mechanism to determine the authentication of users in terms of his overall network, e.g. Capture Portal. There may be legacy clients that try to authenticate with Shared Key while others try to authenticate with Open. It is assumed that the encryption in this case is WEP but the WS410 does not force this.

- In WPA, it is assumed that the basic 802.11 authentication is Open. WPA defines advanced authentications, either PSK (Pre-Shared Key) or RADIUS. In both cases, the initial keys (for broadcast and for unicast traffic) are determined during the last phase of the WPA authentication.

  When RADIUS Authentication is used, the RADIUS server can determine, in addition to the broadcast and unicast keys, the VLAN for the user belongs to (WS410 supports multiple VLANs per SSID).

- The WS410 has the capability to have an SSID that supports both RADIUS and PSK authentication. The exact method is decided according to the packet that comes from the client. If multiple VLANs are defined over such an SSID, a client that is authenticated using PSK gets assigned to the default VLAN, while the clients that authenticate using RADIUS have their VLAN determined by the RADIUS.

Encryption Methods

Legacy 802.11 clients may connect Open (no encryption), or WEP.

In WEP, the encryption key can be either 40bit or 104bit.

In WPA, WS410 supports TKIP encryption.

Since some clients may be legacy (supporting only WEP), WS410 has the capability to have SSIDs that support both WEP and TKIP clients. In this case, the broadcast key is WEP, while the unicast key is either TKIP or WEP, depending on the way the client connected to the system. This mode is called TSN (Transient Security Network). ..

NOTE: When you configure a TSN SSID, configure the WEP key as key #2, since key #1 is used by TKIP.

VLAN Introduction and Configuration

Tagging VLANs

While on the Wireless media the VLANs are identified by different broadcast keys, on the Ethernet interface they are identified by tags. The VLAN tag is added following the Ethernet header.

The default VLAN has the VLAN ID equal to 1. All management traffic to and from WS410 is on this VLAN, however, the traffic that leaves the unit is untagged. The backhaul device (switch or router) is configured to pass all VLANs on the port to WS-410, and VLAN 1 is the default VLAN for this port.

Configuring VLANs

To configure a VLAN

1. Click Security from the menu bar.

   The Security page displays.

2. Click VLANs Mode to enter VLAN mode . A popup asks if you are sure about the move; click OK.

   The Security page appears in VLANs mode (See figure 6.9 below).

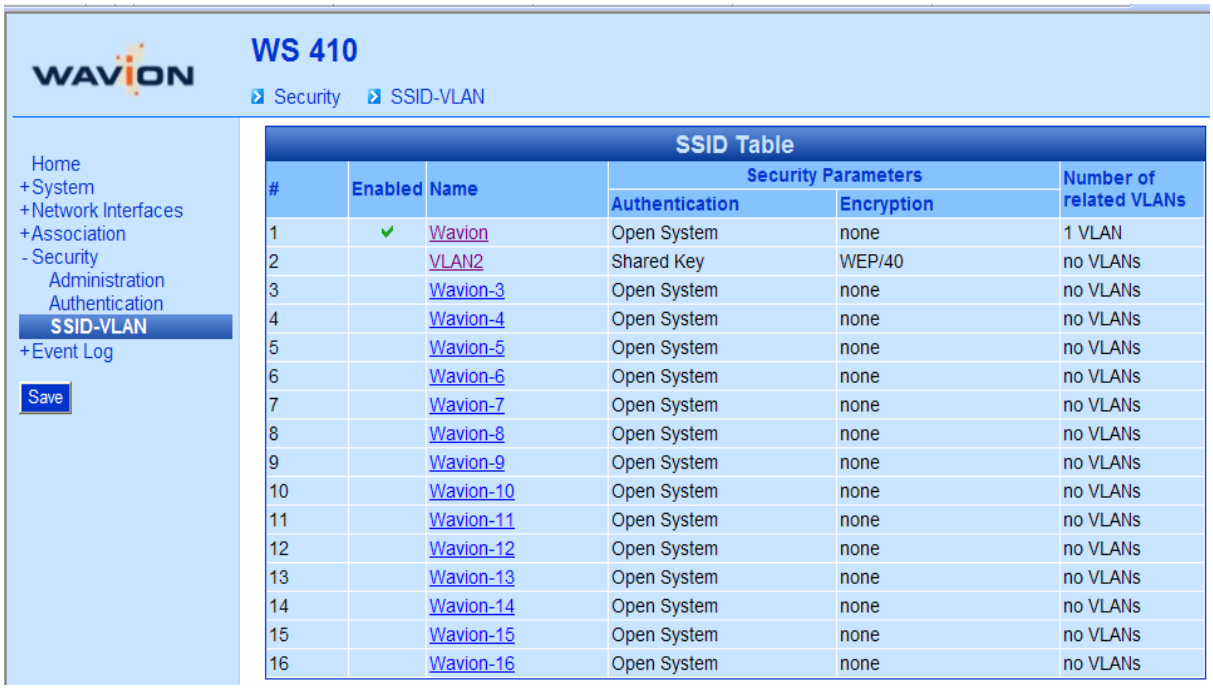
Figure 6.9. **Security Page in VLANs Mode**

3. Select Security>SSID-VLAN from the menu on the left to get the list of pre-defined (and disabled) SSIDs.

   The SSID page is displayed in VLANs mode.

NOTE: The look of the SSID page varies significantly when VLANs are enabled. Throughout the rest of this section the VLAN format is used.

Figure 6.10. **SSID Page in VLANs Mode**

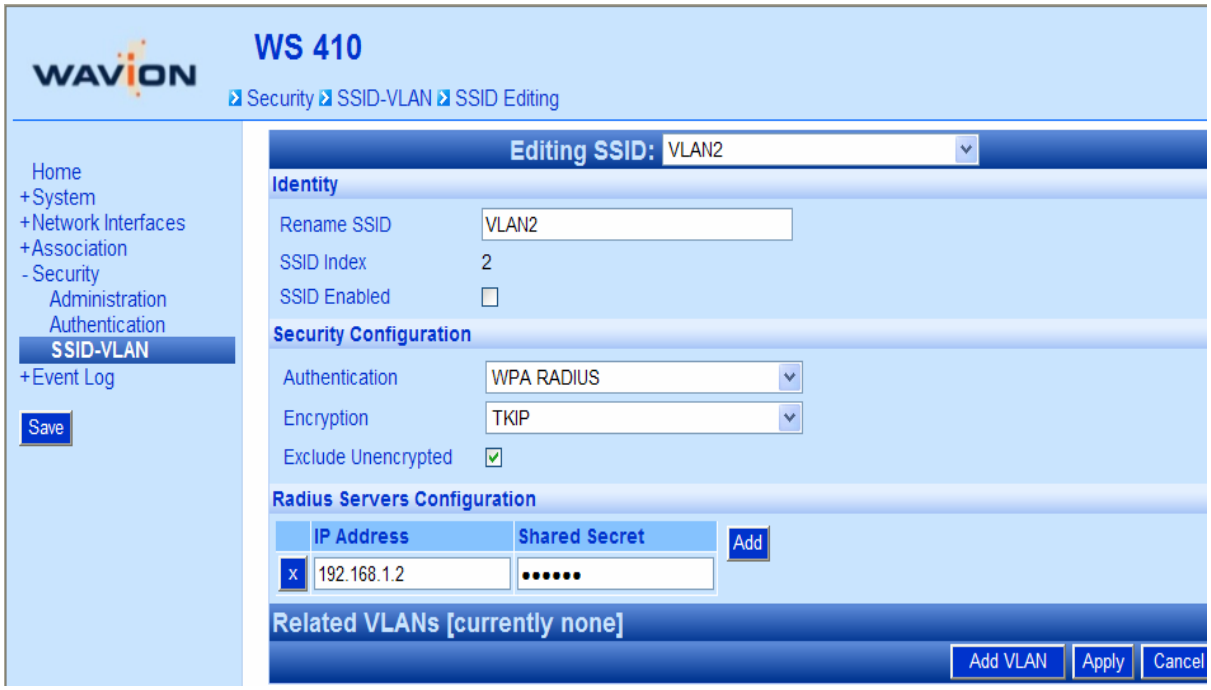

WAVION
WS 410
Security
SSID-VLAN
Home
+System
+Network Interfaces
+Association
-Security
Administration
Authentication
SSID-VLAN
+Event Log
Save
SSID Table
| Enabled | Name | Security Parameters | Number of related VLANs
Authentication | Encryption
1 | ✔ | Wavion | Open System | none | 1 VLAN
2 | | VLAN2 | Shared Key | WEP/40 | no VLANs
3 | | Wavion-3 | Open System | none | no VLANs
4 | | Wavion-4 | Open System | none | no VLANs
5 | | Wavion-5 | Open System | none | no VLANs
6 | | Wavion-6 | Open System | none | no VLANs
7 | | Wavion-7 | Open System | none | no VLANs
8 | | Wavion-8 | Open System | none | no VLANs
9 | | Wavion-9 | Open System | none | no VLANs
10 | | Wavion-10 | Open System | none | no VLANs
11 | | Wavion-11 | Open System | none | no VLANs
12 | | Wavion-12 | Open System | none | no VLANs
13 | | Wavion-13 | Open System | none | no VLANs
14 | | Wavion-14 | Open System | none | no VLANs
15 | | Wavion-15 | Open System | none | no VLANs
16 | | Wavion-16 | Open System | none | no VLANs

The following information is displayed on the SSID Table.

Field	Description
Enabled	Indicates whether the SSID is enabled or not
SSID Name	The full SSID string
Security Parameters	
Security Mode	The specific Security Mode as defined for the SSID.
Authentication	The specific Authentication method as defined for the SSID
Encryption	The specific Encryption method as defined for the SSID.
Number of Related VLANs	The number of VLANs that are related to the specific SSID.

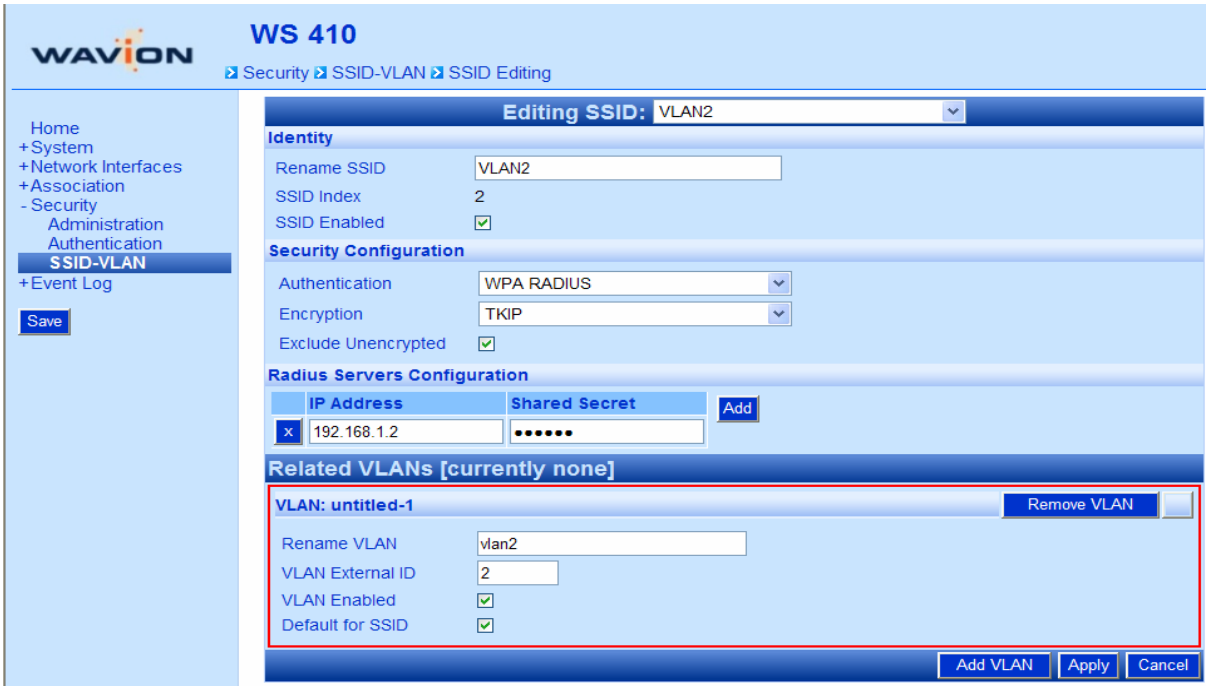
4. Click an SSID name to edit its parameters (e.g. VLAN2) to edit its parameters.

Figure 6.11. **Editing SSID Page**



5. Click Add VLAN at the bottom right of the window to configure the VLAN Parameters. The Add VLAN section of the page is displayed.

Figure 6.12. **Editing SSID Page with Add VLAN Section**



6. In the Rename SSID field, enter an SSID Name to be used in Probe Responses.

NOTE: Only the Primary SSID (the first SSID) is advertised in Beacons. These additional SSIDs are hidden SSIDs.

7. Check the SSID Enabled checkbox. This enables the SSID.
8. Configure all security parameters: Mode, Authentication, and Encryption as required. See on page 76. Keys are added in the Related VLAN section below.
9. Within the Related VLANs edit the VLAN Name and VLAN ID.
10. Edit the VLANSs specific security parameters that are related to the SSID Security definition.
11. Make sure the VLAN and SSID are enabled by marking the VLAN Enabled and SSID enabled checkbox respectively.
12. Click Apply.

Figure 6.13. **Editing SSID Adding VLAN WEP**

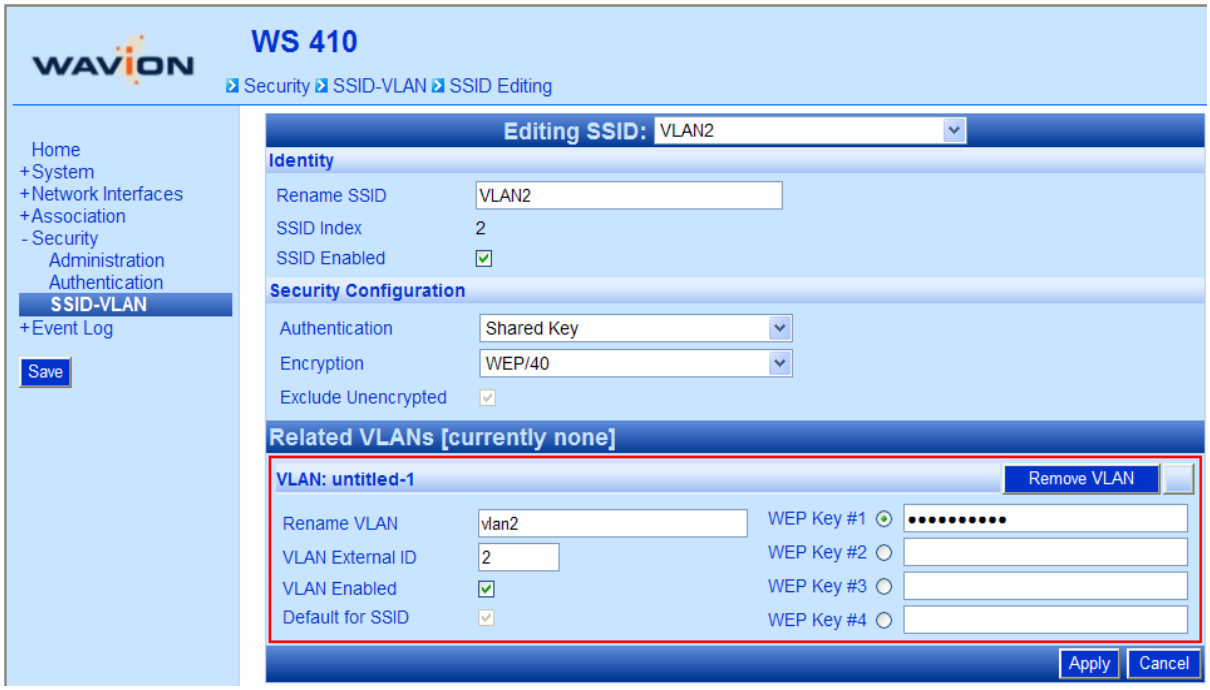
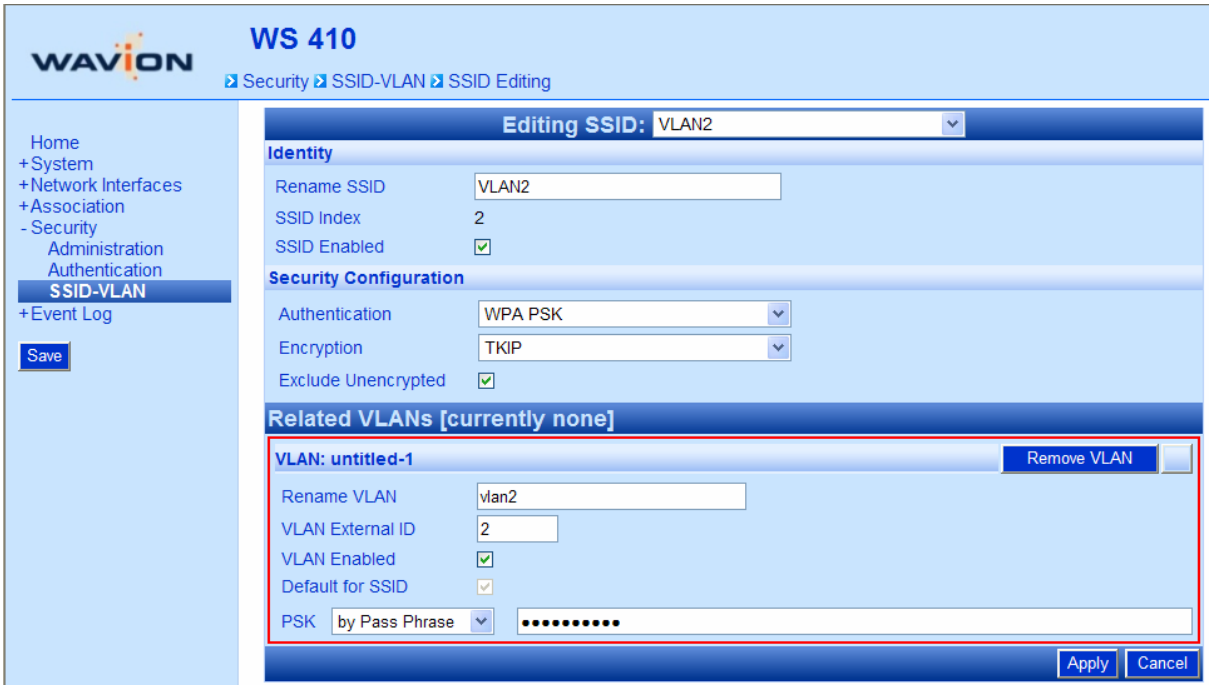


Figure 6.14. **Editing SSID Add VLAN WPA**

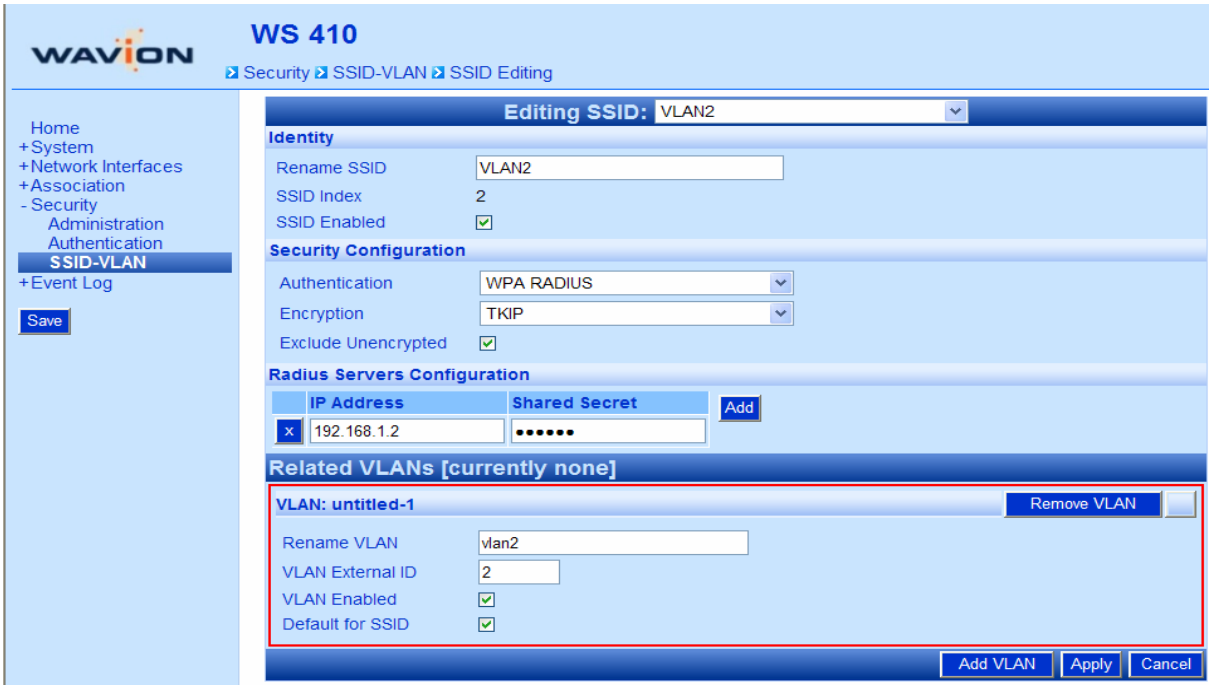


Configuring Multiple VLANS per SSID

The SSID acts as a "security template" - it determines the general security mode (WPA, WEP, etc.). The Security details (the keys themselves) are linked to the VLAN. Therefore, there is an option to assign multiple VLANs to the same "security template" which is the SSID. This option is applicable only when another authority (i.e. RADIUS Server that supports VLAN assignment) is involved in the Authentication process. The RADIUS can determine the exact VLAN that the connecting client is bound to after the Authentication process is completed.

Configuring RADIUS Assigned VLANS

Figure 6.15. **Editing SSID with RADIUS -- Multiple VLANs**



1. Perform steps 1-7 in Configuring VLANs on page 70 above.
2. Under Security Configuration, under Authentication, if you select WPA RADIUS or WPA PSK + RADIUS you enable RADIUS authentication. In this case, there is an option to edit multiple VLANs, one after the other. There can be up to 16 VLANs in the overall system.
3. Only one VLAN has the Default for SSID checkbox marked. This indicates to the WS410 which is the default VLAN when authentication on the SSID is performed and the RADIUS does not provide the assignment to VLAN (due to possible configuration problems in the RADIUS).

   Make sure you configure the RADIUS server to handle clients on multiple VLANs.

   Make sure that access to the RADIUS Server, including the Shared Secret, is configured correctly. See Configuring RADIUS Server Parameters: Server Manager Tab on page 60

Security Modes: Authentication and Encryption Methods

The following are the different combinations of security modes.

Security Mode	Authentication Mode	Encryption Mode
None	Open system	None
WEP	• Open system • Shared key • Open system + Shared key	• WEP/40 • WEP/104
WPA	• PSK (Pre-shared key) • Radius • PSK + Radius	• TKIP • TKIP+WEP/40 • TKIP+WEP/104

Authentication Combinations

WS410 allows authentication of various types and in various combinations.

- The basic 802.11 authentications are Open (none) and Shared Key. In Shared Key Authentication, the WEP key is used as the shared key.

  If the SSID is configured to Open + Shared Key, this means that both types of clients can associate to the AP. This can be useful when the IT has another mechanism to determine the capabilities or authentication of users in terms of his overall network, e.g. Capture Portal. There may be legacy clients that try to authenticate with Shared Key while others try to authenticate with Open. It is assumed that the encryption in this case is WEP but WS410 does not force this.

- In WPA, it is assumed that the basic 802.11 authentication is Open. WPA defines advanced authentications, either PSK (Pre-Shared Key) or RADIUS. In both cases, the initial keys (for broadcast and for unicast traffic) are determined during the last phase of the authentication.

  When RADIUS Authentication is used, the RADIUS can determine the VLAN that the user gets (we support multiple VLANs per SSID), if the IT wants it.

- WS410 has the capability to have SSIDs that support both RADIUS and PSK authentication. The exact method is decided according to the packet that comes from the client. If multiple VLANs are defined over this SSID, a client that is authenticated using

PSK gets assigned to the default VLAN, while the clients that authenticate using RADIUS have their VLAN determined by the RADIUS.

Encryption Methods

Legacy 802.11 clients may connect Open (no encryption), or WEP.

In WEP, the encryption key can be either 40bit or 104bit.

In WPA, WS410 supports TKIP encryption.

Since some clients may be legacy (supporting only WEP), WS410 has the capability to have SSIDs that support both WEP and TKIP clients. In this case, the broadcast key is WEP, while the unicast key is either TKIP or WEP, depending on the way the client connected to the system. This mode is called TSN (Transient Security Network).

When you configure a TSN SSID, configure the WEP key as key #2, since key #1 is used by TKIP.

SSIDs and VLANs

In WS410, the SSID has the notion of Security definitions. All SSIDs (with their Security capabilities) are advertised in probe responses. The primary SSID is also advertised in the Beacon.

An AP transmits beacons (every beacon interval) in which it advertises the primary SSID. In addition, when a client sends a Probe Request with the correct SSID (may be different from the Primary SSID), the AP responds with the matching Probe Response it exists).

In case VLANs configuration is required, the user has to define the SSIDs in the WS410, and to define the specific SSID to which each client needs to connect, in the client's configuration tool (which is out of scope of this user manual).

In VLANs mode, when clients are associated to an SSID, they are assigned to the default VLAN that is linked to this SSID. When RADIUS is used for authentication, the RADIUS can determine the exact VLAN for the user (among all VLANs that are linked to this SSID).

CHAPTER 7

Viewing Events

You can view and configure logs of system events.

Viewing the Most Recent Events

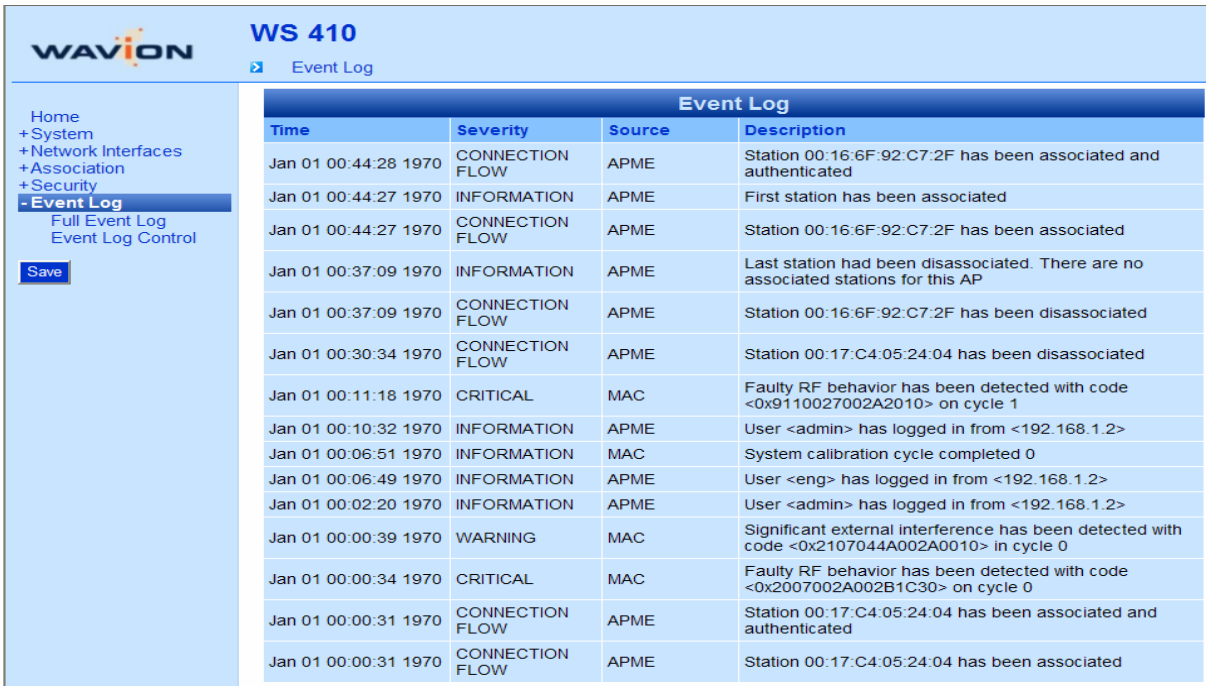
The Event Log page displays the systems most recent events.

To display the event log

- Click Event Log in the menu.

  The log of most recent system events displays.

Figure 7.1. **Event Log**



Event Log

Time	Severity	Source	Description
Jan 01 00:44:28 1970	CONNECTION FLOW	APME	Station 00:16:6F:92:C7:2F has been associated and authenticated
Jan 01 00:44:27 1970	INFORMATION	APME	First station has been associated
Jan 01 00:44:27 1970	CONNECTION FLOW	APME	Station 00:16:6F:92:C7:2F has been associated
Jan 01 00:37:09 1970	INFORMATION	APME	Last station had been disassociated. There are no associated stations for this AP
Jan 01 00:37:09 1970	CONNECTION FLOW	APME	Station 00:16:6F:92:C7:2F has been disassociated
Jan 01 00:30:34 1970	CONNECTION FLOW	APME	Station 00:17:C4:05:24:04 has been disassociated
Jan 01 00:11:18 1970	CRITICAL	MAC	Faulty RF behavior has been detected with code <0x9110027002A2010> on cycle 1
Jan 01 00:10:32 1970	INFORMATION	APME	User <admin> has logged in from <192.168.1.2>
Jan 01 00:06:51 1970	INFORMATION	MAC	System calibration cycle completed 0
Jan 01 00:06:49 1970	INFORMATION	APME	User <eng> has logged in from <192.168.1.2>
Jan 01 00:02:20 1970	INFORMATION	APME	User <admin> has logged in from <192.168.1.2>
Jan 01 00:00:39 1970	WARNING	MAC	Significant external interference has been detected with code <0x2107044A002A0010> in cycle 0
Jan 01 00:00:34 1970	CRITICAL	MAC	Faulty RF behavior has been detected with code <0x2007002A002B1C30> on cycle 0
Jan 01 00:00:31 1970	CONNECTION FLOW	APME	Station 00:17:C4:05:24:04 has been associated and authenticated
Jan 01 00:00:31 1970	CONNECTION FLOW	APME	Station 00:17:C4:05:24:04 has been associated

The following fields appear on the Event Log page:

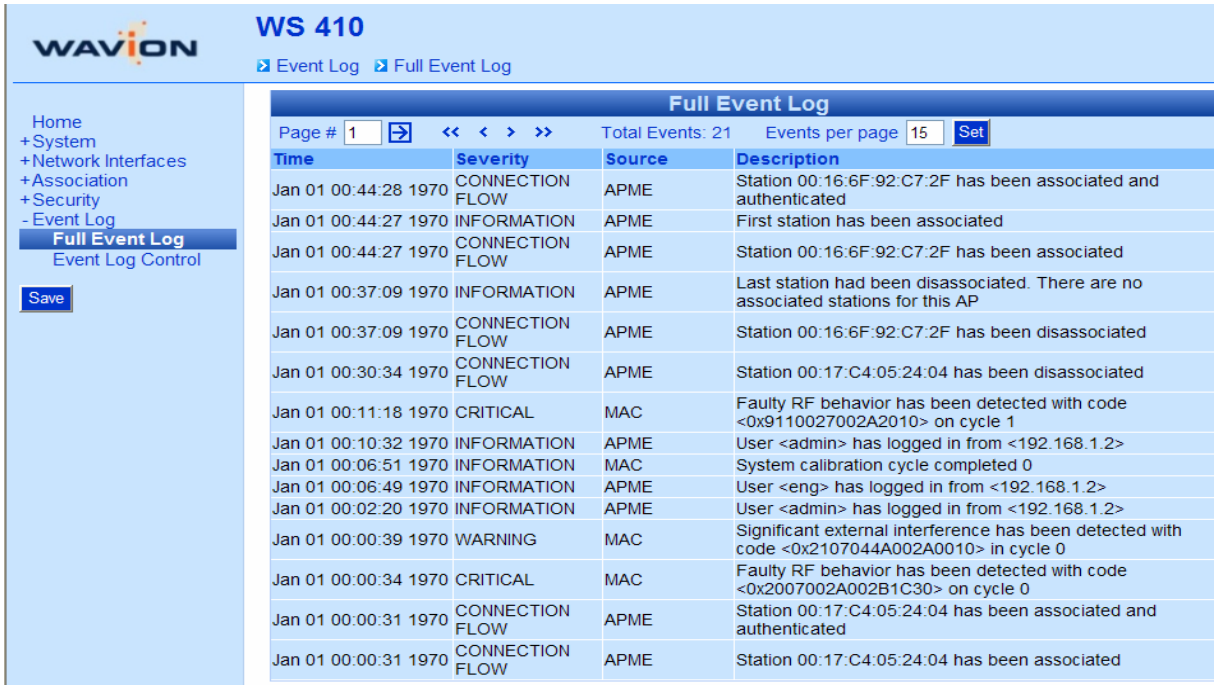
Table 7.1. **Event Log page**

Field	Description
Time Since Uptime	The time the event occurred. The time of 0 is the time the system was last rebooted.
Severity	The severity of the event showing how serious event is: Information, Connection Flow, Warning, Critical, or the event type (e.g. Connection Flow)
Source	System module reporting the event
Description	Complete description of circumstances of event

Viewing the Full Event Log

Clicking the Full Event Log menu item displays the Full Event Log page. This page displays all the events in the internal log file since the system was rebooted or since the file was overwritten. At the top of the page are controls allowing you to navigate through the pages, and select how many events are shown per page.

Figure 7.2. **Full Event Log Page**


WAVION
WS 410
Event Log
Full Event Log
Home
+System
+Network Interfaces
+Association
+Security
- Event Log
Full Event Log
Event Log Control
Save
Full Event Log
Page # 1
Total Events: 21
Events per page 15
Set
Time
Severity
Source
Description
Jan 01 00:44:28 1970 CONNECTION FLOW APME Station 00:16:6F:92:C7:2F has been associated and authenticated
Jan 01 00:44:27 1970 INFORMATION APME First station has been associated
Jan 01 00:44:27 1970 CONNECTION FLOW APME Station 00:16:6F:92:C7:2F has been associated
Jan 01 00:37:09 1970 INFORMATION APME Last station had been disassociated. There are no associated stations for this AP
Jan 01 00:37:09 1970 CONNECTION FLOW APME Station 00:16:6F:92:C7:2F has been disassociated
Jan 01 00:30:34 1970 CONNECTION FLOW APME Station 00:17:C4:05:24:04 has been disassociated
Jan 01 00:11:18 1970 CRITICAL MAC Faulty RF behavior has been detected with code <0x9110027002A2010> on cycle 1
Jan 01 00:10:32 1970 INFORMATION APME User <admin> has logged in from <192.168.1.2>
Jan 01 00:06:51 1970 INFORMATION MAC System calibration cycle completed 0
Jan 01 00:06:49 1970 INFORMATION APME User <eng> has logged in from <192.168.1.2>
Jan 01 00:02:20 1970 INFORMATION APME User <admin> has logged in from <192.168.1.2>
Jan 01 00:00:39 1970 WARNING MAC Significant external interference has been detected with code <0x2107044A002A0010> in cycle 0
Jan 01 00:00:34 1970 CRITICAL MAC Faulty RF behavior has been detected with code <0x2007002A002B1C30> on cycle 0
Jan 01 00:00:31 1970 CONNECTION FLOW APME Station 00:17:C4:05:24:04 has been associated and authenticated
Jan 01 00:00:31 1970 CONNECTION FLOW APME Station 00:17:C4:05:24:04 has been associated

The following fields appear on the Full Event Log page:

Table 7.2. **Full Event Log page**

Field	Description
Total Eventst	Number of total events in log
Events per page	Number of events shown per page; modifiable
Page navigator	Allows paging through log
Time Since Uptime	The time the event occurred. A time of 0 is the time the system was last rebooted
Severity	The severity of the event, showing how serious event is: Information, Warning, Critical, or the event type (e.g. Connection Flow)
Source	The system module reporting the event
Description	Complete description of circumstances of event

Navigating the Event Log

The following is the description of the buttons used to navigate the event log.

The description of the keys controlling the Full Event Log page:

Table 7.3. **Viewing the Full Event Log page**

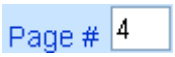
Key	Description
Page# 	Indicated the number of the page that is currently viewed. The user may type the desired page # directly without the need to scroll through all pages.
Arrow in square mark	is an Enter button. It is used to effect the change of the page number entered by the user.
Arrows to the Left or Right	are used as scrolling buttons. An arrow to the right is forward (older), and an arrow to the left is backwards(newer). Note that the going forward in the file means that old events are displayed. One arrow indicates simple forward or backward. Two arrows jumps directly to the first or last page.

Table 7.3. **Viewing the Full Event Log page**

Key	Description
Event Count Event's count :120	indicates the total number of events that are in the internal file
Events per page Events per page 5	The number of events shown on a page. The user my change this value and hit the Arrow-in-a-square to activate the change. By default, there are 15 events per page.

Configuring Event Logs

You can configure what appears in the event log, and what is sent to the external logs, such as SYSLOG and SNMP Trap Manager, through the Event Log Control page. On this page, you can control parameters relating to the event log, such as what types of events included in the log, and what method is used to collect the events.

To configure event logs

1. Click Event Log and then Event Log Control in the menu.
   The Event Log Control page displays.

Figure 7.3. **Event Log Control Page**

The following fields appear on the Event Log Control page.

Table 7.4. **Event Log Control page**

Field	Description
Action	Select the severity levels/types of events logged by each type of event information collection mechanism
Log to buffer	Events marked in this row are logged to the internal buffer
Send SNMP trap	Events marked in this row are sent to the SNMP trap manager
Send SysLog	Events marked in this row are sent to the SysLog server
Severity Level Events	Select the types of events to be saved to each log
Critical Errors	
Warning Events	
Information Events	
Type Events	
Connection Flow Events	Indicates whether connection flow events are saved to a log or sent to a remote server.
Event Log Buffer Size[Kbytes]	Maximum size of the internal log; events reaching log when the buffer is full overwrites over the oldest events
IP Address of SNMP Trap Destination (NMS)	The IP Address of the SNMP Server.
IP Address of Syslog Server	The IP Address of the SYSLOG Server to which SYSLOG events are to be sent.
Options	
Apply	Click to have your changes take effect temporarily
Save	Click to have your changes remain in effect after a reboot
Cancel	Click to clear your changes; this is only possible if Apply or Save were not clicked

2. You can modify selections on this page.
3. Click Apply to save changes temporarily.
4. Click Apply and Save to have changes remain in effect after a reboot.

CHAPTER 8

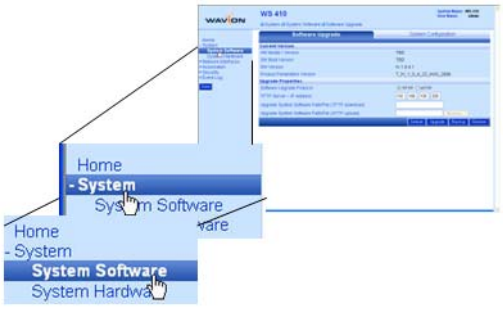
Upgrading the System Software

From time to time there are revisions of the software. This section explains how to upgrade the software in your system.

To upgrade the embedded software in WS410

1. Log in to the management system through a web browser. Login instructions are available in the printed quick start guide and in the login section of the manual.

Figure 8.1. **Getting to Software Upgrade Tab**



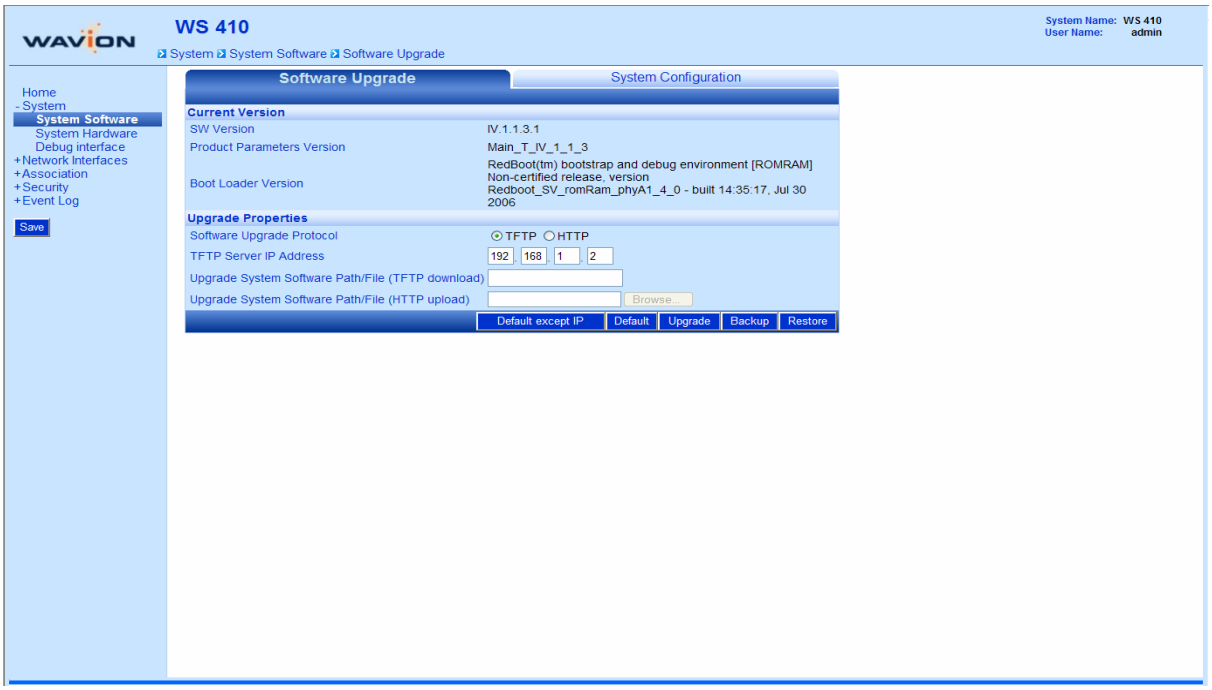
2. Click System on the menu bar.

   Menu sub-items appear.

3. Then click System Software.

   The Software Upgrade tab is displayed.

Figure 8.2. **Software Upgrade Tab**



4. In the Upgrade Properties area, in the Software Upgrade Protocol field, select either the TFTP or HTTP radio button.
5. If you select the TFTP radio button enter the TFTP Server IP Address and the System Software Path/File (TFTP upload) in the appropriate fields.
6. If you select the HTTP radio button, in the Upgrade System Software Path/File (HTTP upload) field, click Browse.

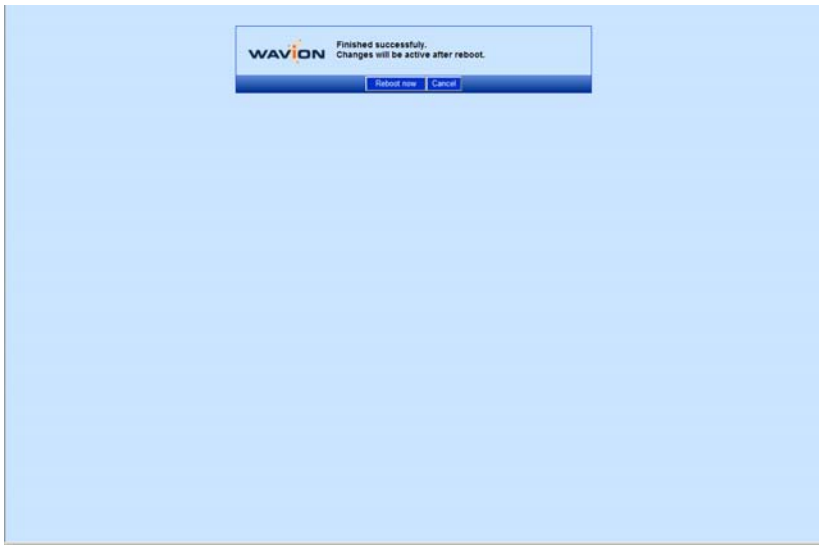
   The Choose file dialog is displayed.

   Select the appropriate file to upload in the Choose file dialog. The appropriate file has the extension of ".wj".

   Click Open.
7. Click Upgrade at the bottom of the Software Upgrade tab.

   The time to upload the software depends on the complexity of the network between the downloading host and the WS410 unit. In a simple network, it takes about one minute to upload the software. When it completes, a popup is displayed

Figure 8.3. **Done Successfully Popup**

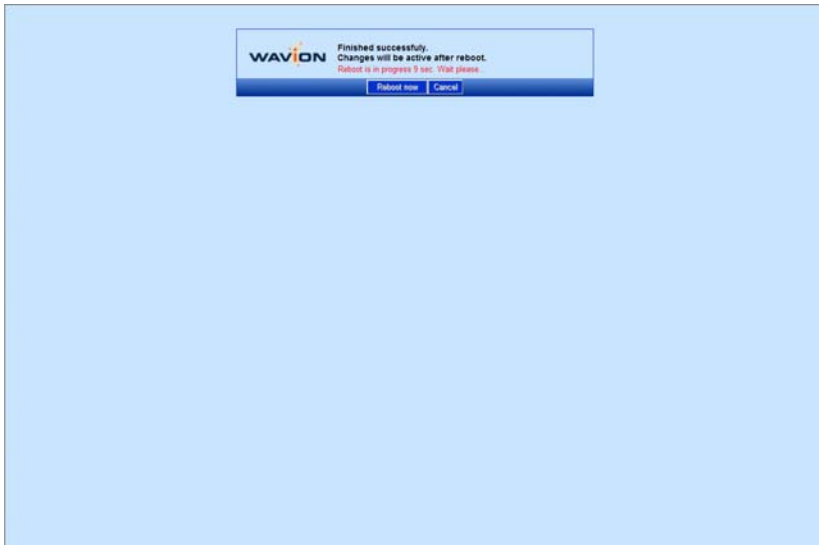


For the upgrade to take effect, the system must be rebooted.

8. Click Reboot Now.

A popup is displayed.

Figure 8.4. **Reboot in Progress**



9. After Reboot is complete, the WEB GUI automatically brings you back to SW Upgrade tab, see Figure 8.2. The new software version is shown

CHAPTER 9

Appendix: Quick Start Guide to Wavion WS410

This section explains how to quickly get started using the Wavion WS410. The intended audience for this guide is trained technical professionals. The following topics are covered in this guide:

- Introduction
- Connecting the WS410 to a PC
- Log In
- Becoming Oriented with the Application
- Modifying the System Configuration
- Changing the Network Interface Configuration
- Automatic Channel Selection
- Modifying the Security Configuration
- Rebooting the System

Introduction

The Wavion WS410 was designed so that it works straight “out-of-the-box”. It can start operating without any configuration changes. However, we advise that you make some configuration changes that affect the wireless security and networking settings before testing.

This quick start guide directs you to the specific parameters that you need to change.

Connecting the WS410 to a PC

You must connect the WS410 to a PC.

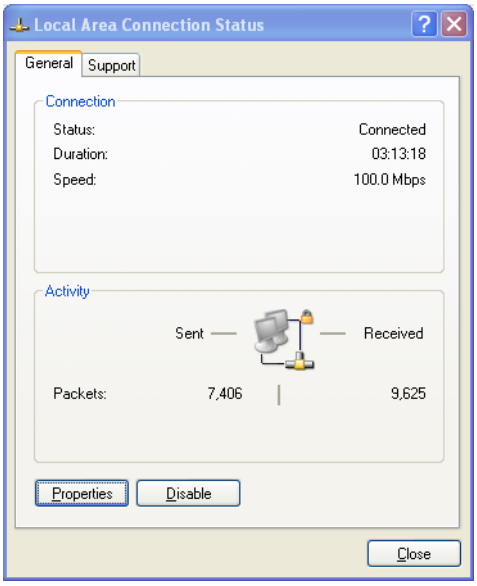
To connect the WS410 to a PC

1. Connect the WS410 to a source of electricity.
2. Connect the WS410 to the local area connection port of the PC.
3. Right-click the Local Area Connection icon in the notification area (system tray).

   A menu is displayed.

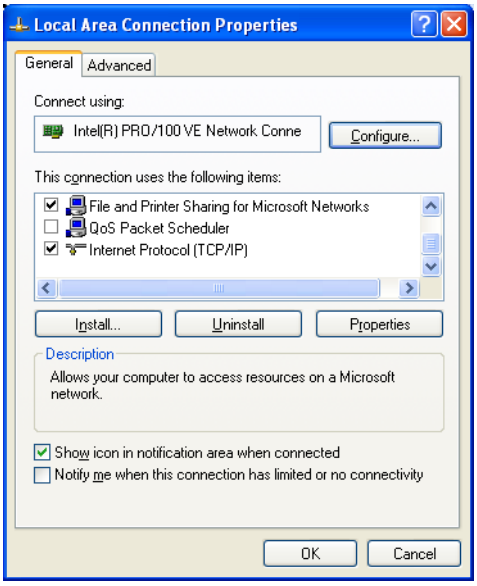
4. Click Status on the menu.

   The Local Area Connection Status dialog is displayed.



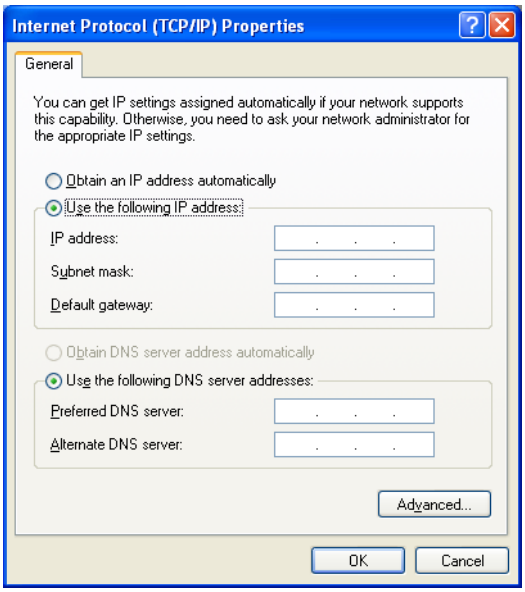
5. Click Properties.

   The Local Area Connection Properties dialog is displayed.



6. Scroll down to Internet Protocol TCP/IP and double-click.

The Internet Protocol (TCP/IP) Properties dialog is displayed.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

7. Select “Use the following IP address”.
8. In the IP address field, enter 192.168.1.2.
9. In the IP mask field, enter 255.255.255.0.
10. Click OK. Close all LAN dialogues.

Log In

After the WS410 is connected to a PC, you need to log in.

To log in

1. Open the web browser.
2. Enter the IP address in the address bar. Default is 192.168.1.1.

   The login dialog is displayed.

Figure 9.1. **Login dialog**

3. Enter your user name. The default user name is admin.
4. Enter the password. The default password is admin.

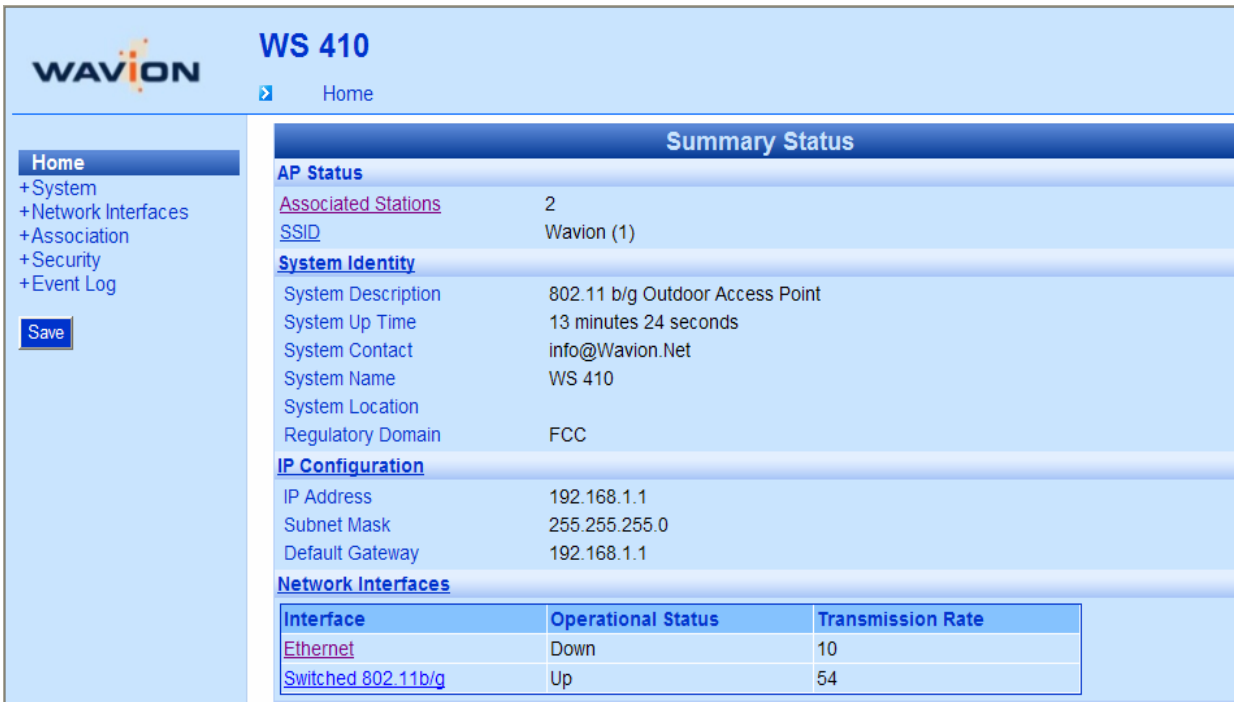
NOTE: User name and password are case sensitive.

NOTE: Once you log in, you can change the user name and password from the Management Configuration screen. Click Security> Administration on the menu bar.

5. Click OK.

   The Home -- Summary Status page appears.

Figure 9.2. **WS410 Home Page**



Becoming Oriented with the Application

The Home page displays a summary of system data and links to other pages that allow management of this data. For the purposes of this quick start, you are instructed how to move from the Home page to the pages where the changes recommended in this guide are made. The pages, including the Home page, can also be reached from the menu bar.

The Home page is displayed on login, and like the other pages of the WS410, comprises the following main sections: a menu bar, a header, and a main page area.

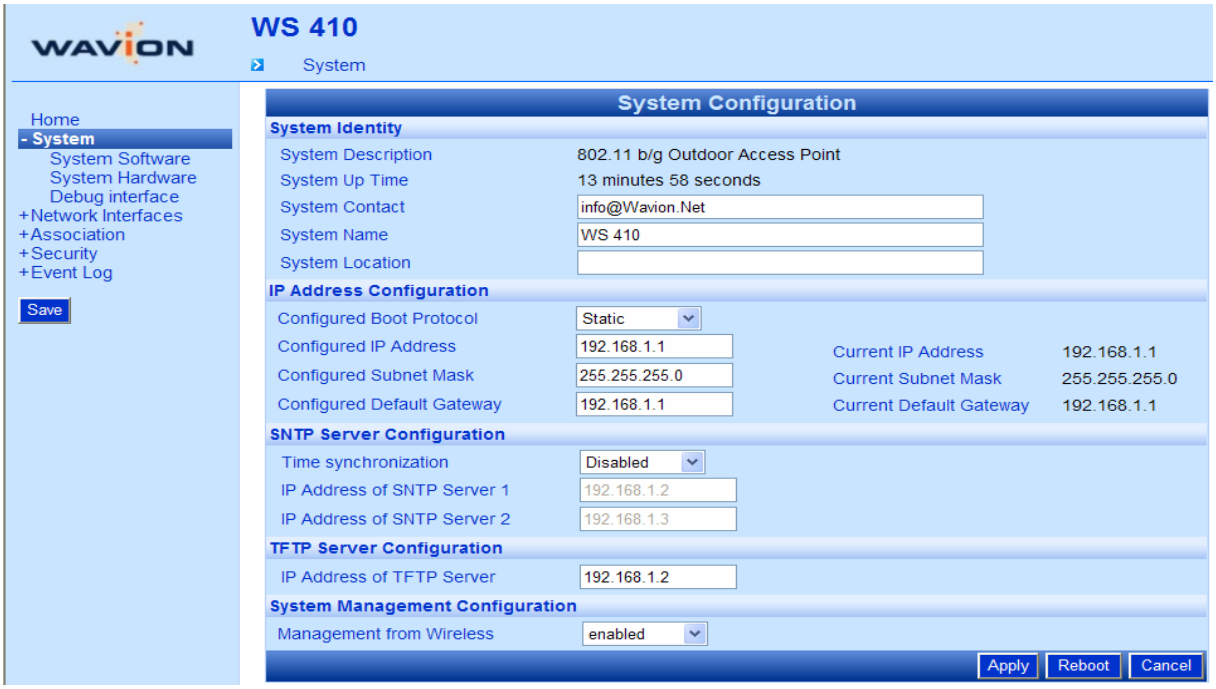
- The menu bar is located on the left side of the screen. This area works like a directory tree; clicking a menu item either causes a different page to be displayed, or causes menu sub-items to appear, from which you can choose the page you are looking for.
- The header contains the system name and user name, and also displays the path to the page. For example, the Home page is reached directly from the menu item Home, so only the word Home is displayed, but when it is necessary to click through additional items on the menu bar in order to reach a page, all these menu items are listed in order in the header.
- The main page area is specific to the functionality of each particular page.

Modifying the System Configuration

From the Home page, click System Identity. (You can also get to this page by clicking System from the menu bar.)

The System Configuration page is displayed.

Figure 9.3. **System Configuration Page.**



This page contains basic static information on the system, such as contact details, and IP addresses. Several changes are recommended on this page.

Setting System Contact Details

In the System Identity area, in the System Contact field, enter the contact E-mail address of the NOC or network owner.

Setting the IP Address Configuration

Change the IP address to allow the full configuration. The Current IP Address Configuration area lists a default IP address; it is possible to perform initial testing with this address, but it is highly recommended to change the IP address. The default IP Address of the unit from the box is 192.168.1.1 using /24 bit mask.

To change the IP address

In the Configured IP Address Configuration section,

1. To allow entry of a new IP address, select Static from the Configured Boot Protocol dropdown list.
2. In the Configured IP Address field, enter the required IP address.

NOTE: The system must be rebooted for these changes to take effect; for the quick start, you are instructed to reboot after the quick start procedure is completed.

Setting the System Management Configuration

You can decide to allow system management from the Wireless Interface, or to allow management only from the Ethernet Interface, for security purposes.

To enable or disable system management from the Wireless Interface

In the System Management Configuration area, in the Management from Wireless field, from the dropdown list, select Enabled to allow system management from the wireless interface, or Disabled to restrict system management to the Ethernet Interface.

Saving Changes

NOTE: After making changes on a page, you must click both Apply and Save, or the changes do not remain in effect after the next reboot.

To have changes remain in effect

1. Click Apply.
2. Click Save.

Return to the Home page from the menu bar to continue with the quick start procedure.

Changing the Network Interface Configuration

From the Home page, in the Network Interfaces area, click Switched 802.11 b/g. (You can also get to this page from the Network Interfaces item on the menu.)

The Switched 802.11 b/g page is displayed.

Figure 9.4. **Switched 802.11 b/g Page**

On this page you can configure the wireless interface. There are several recommendations for this page.

Setting the Operational Channel

Operational channels should be set up in such a way that if you have multiple units, they interfere with each other as little as possible. If you have up to three units, it is recommended to use channels 1, 6, and 11, as that minimizes interference between the channels.

To set the Operational Channel

In the Status and Configuration area, from the dropdown list in the Operational Channel field, select the channel on which the system runs. Default is Channel 6: 2437 MHz.

Setting the Transmission Power

Be sure the Transmission Power is set to the maximum; Maximum Tx Power = 1 and Minimum Tx Power = 6, it's a 3dB steps with the dynamic range of 15dB.

Dynamic Interference Handling

Refer to Chapter 4 for definition. The DIH provides which Channel to use based on he Total CCA Activity and the Noise Level. These values are only valid seven minutes after reboot and when the First System Calibration is complete. It can be configured Dynamically or Static Mode.

Saving Changes

1. Click Apply.
2. Click Save.

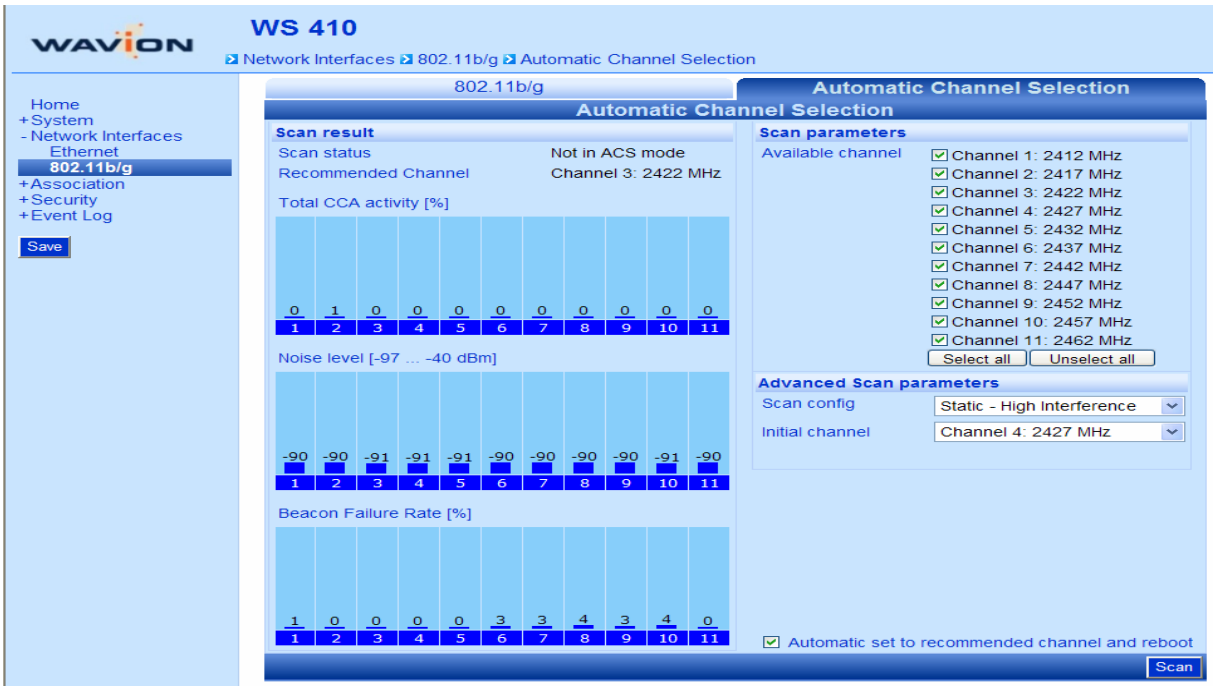
   You are warned that it is necessary to reboot before the changes take effect. We will do this at the end of the quick start.

Click Home to return to Home page to continue the quick start procedure.

Automatic Channel Selection

The Automatic Channel Selection (ACS) is a tool to select the best channel based on the activity and the interference level at each channel by scanning the frequency channel.

Figure 9.5. **Automatic Channel Selection page**



Modifying the Security Configuration

To display the Editing SSID page

- On the Home page, in the AP Status area, click SSID.

  The Editing SSID page is displayed.

Figure 9.6. **Editing SSID**.

This page allows management of the security configuration. There are several changes recommended on this page.

Renaming the SSID

In the Rename SSID field, enter the correct SSID for the network of users to be served.

NOTE: The SSID is case sensitive and shorter than 32 characters.

Setting the Security Mode

In the Security Mode field, you can initially set the value as None (default) to have the system completely open.

Setting the Authentication Type

In the Authentication field, select from the dropdown list; default is Open System.

Setting the Encryption Type

In the Encryption field, from the dropdown list; default is None.

Saving Changes

1. Click Apply.
2. Click Save.

Rebooting the System

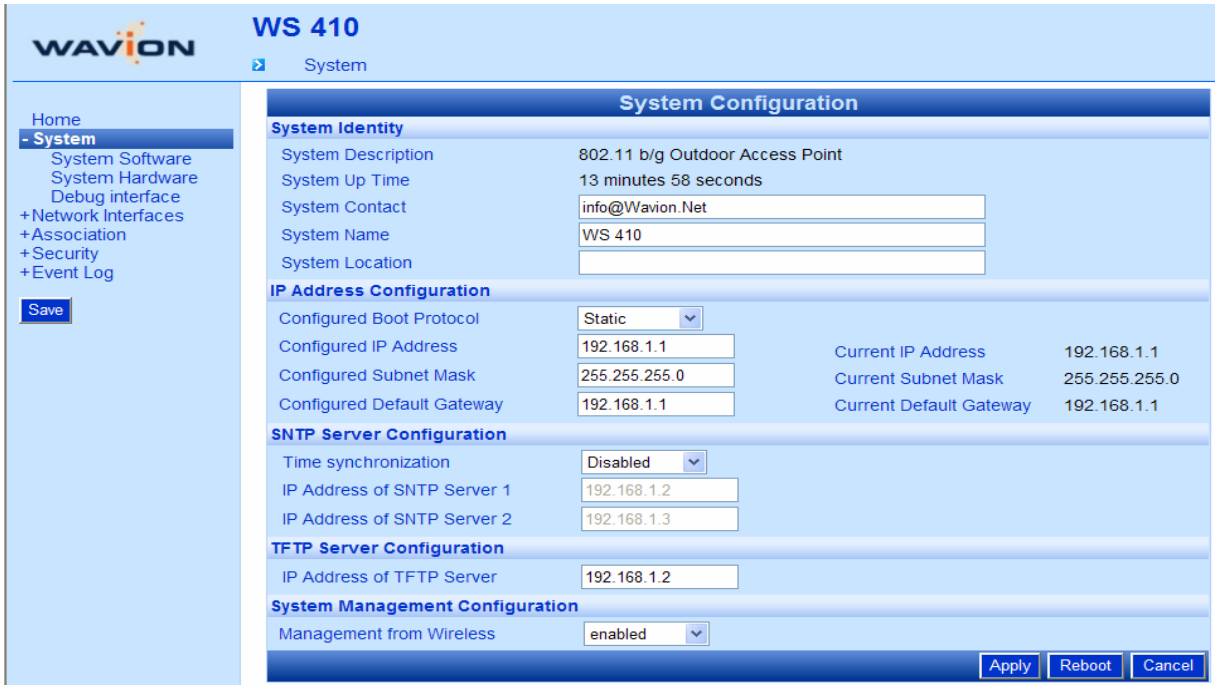
Several of the changes made during the quick start procedure require rebooting to take effect. After completing the procedure, reboot the system.

To reboot the WS410

1. From the menu, click System.

   The System Configuration page displays.

Figure 9.7. **System Configuration Page**



2. Click Reboot.

   This system reboots and puts into effect all changes that were made and required reboot. It takes about one minute for the system to come back up again after reboot.

Congratulations!

You have now completed the quick start procedure. We hope you enjoy your experience with the WS410 and provide a reliable wireless networking experience to your customers.

CHAPTER 10

Appendix: Troubleshooting

We hope your experience with the WS410 is as smooth as possible. In this section we provide tips to solve some common problems.

Problem	Solution
Unable to Ping or HTTP the New Unit	• Check the Power • Is the AP Operational? Check the LED, make sure it showing Green on the Status • WS410 default IP Address is 192.168.1.1 /24 mask
Client unable to acquire an IP Address from DHCP Server	• Is the AP Operational? • Check the DHCP Server. Use Static IP to test the DHCP configuration • Check for Interference. Noise level should be around -97dBm to -82dBm
Clients experiencing low throughput	• Check for Interference. Noise level should be around -97dBm to -82dBm • Check the clients modulation rate e.g 54Mbps, 38Mbps, 11Mbps....